



## News Release

October 14, 2006

### BANK OF JAMAICA

#### **ANTI-MONEY LAUNDERING (AML) POLICY COMBATTING THE FINANCING OF TERRORISM (CFT) POLICY**

---

1. The objective of the Bank of Jamaica's AML/CFT Policy is to assist the Central Bank with implementing the mandate to ensure that its facilities are not used in the commission of, or to further the commission of, financial crimes particularly money laundering or the financing of terrorist activities. This policy therefore establishes guidelines for the management and employees of the Central Bank as regards their expected roles in the AML/CFT procedures that have been and which continue to be implemented.
2. This policy has been prepared against the background of the functions and objectives of the Central Bank, and also with regard to the customer profile and by extension the AML/CFT risks to which the Central Bank may be subject by virtue of its operations and the persons/institutions with which it conducts business.

Section 5 of the Bank of Jamaica Act outlines the general objectives of the Central Bank as follows:-

- To issue and redeem notes and coins,
- To keep and administer the external reserves of Jamaica,
- To influence the volume and conditions of supply of credit so as to promote the fullest expansion in production, trade and employment, consistent with the maintenance of monetary stability in Jamaica and the external value of the currency,

- To foster the development of money and capital markets in Jamaica, and
- To act as banker to the Government.

The pursuit of the above objectives is executed through a number of functions which include:-

- ❖ Monetary policy decision-making inclusive of the setting of inflation targets and maintenance of Net International Reserves (NIR);
- ❖ Monitoring the money and foreign exchange markets with a view to assuring price stability;
- ❖ Supervision and regulation of the banking system, licensed deposit-takers and foreign exchange traders, inclusive of Cambios/Bureaux de Changes and Money Transfer and Remittance Agents and Agencies;
- ❖ Fiscal Agency services to the Government (which includes administering the primary issues of Government securities and debt issues);
- ❖ Banking transactions with customers of the Central Bank.

**2.1** It is recognized that only a portion of the participants in the financial system are direct counterparts with the Central Bank. These are:-

- Central Government;
- Commercial banks (as participants of the clearing system);
- Primary Dealers (as the inter-facers in the market between secondary participants in Government of Jamaica (GOJ) Instruments and BOJ

Instruments and wholesalers of foreign currency sold to the market by the Central Bank);

- Overseas correspondent banks;
- Employees of the Bank of Jamaica;
- Members of the public who:
  - Are direct holders of GOJ instruments or BOJ instruments;
  - Are changing out coins for notes;
  - Are surrendering notes and coins that are no longer in circulation;
  - Are replacing torn or mutilated notes for new notes;
  - Are conducting foreign currency transactions (such as the acquisition of bank drafts; or the purchase or sale of foreign currency for private use and not as a business or for investment purposes).

Notwithstanding the relatively restricted level of its interfaces, the Central Bank is cognizant of the possibility that its services could still be exposed to the risk of money laundering and of other persons wishing to use the Central Bank to facilitate the commission of some other financial crime. Consequently, from the early 1990s, following the signing of the Vienna Convention and the issue of the “Basel Statement of Principles on the Prevention of the Criminal Use of the Banking System”, the Central Bank took steps to ensure that, in addition to issuing Anti-Money Laundering Guidance Notes to the banking community, its own operations would be governed by those principles and subject to the anti-money laundering systems contained in local legislation and international best practice standards.

This initially included:

- The Money Laundering Act 1996
- The Money Laundering Regulations, 1998
- The Bank of Jamaica AML/CFT Guidance Notes
- The CFATF 19 Recommendations
- The FATF 40 + 8 Recommendations
- The Basel Customer Due Diligence

With the passage of the Terrorism Prevention Act in 2005 and the addition of a ninth special recommendation to the FATF Special Recommendations, the Central Bank is taking the steps necessary to ensuring its compliance with these new laws and new FATF requirements.

### **3. Money Laundering and Other Financial Crimes**

As can be seen from the above, the customer profile for the Central Bank is not the same as those for commercial financial institutions that are participants in the banking and wider financial system, and as such it means that the risks to the Central Bank are therefore not quite the same. In the Central Bank's case the customer profile is not only limited but largely comprises persons/institutions that are currently subject to local statutory and global standard AML/CFT obligations and in the case of central government, the additional obligations of anti-corruption laws<sup>1</sup>. As regards other persons named above with whom the Central Bank conducts business, the main risks include:

- Use of the Central Bank's instruments or market intervention sale or purchase of foreign currency to manipulate the exchange rate;
- Transactions attempted with counterfeit notes;
- Transactions attempted with forged signatures;

---

<sup>1</sup> The Corruption Prevention Act, 2002 requires public servants earning above a certain income bracket to file annual asset declarations with the Corruption Prevention Commission.

Transactions conducted with overseas counterparts that may have facilitated a financial crime or which are subject to AML/CFT investigations by the regulator in the overseas jurisdiction;

Corrupt or dishonest employees;

### **3.1 Money Laundering**

The term 'money laundering' refers to all procedures, methods, and transactions designed to change the identity of illegally obtained money so that it appears to have originated from a legitimate source<sup>2</sup>.

### **3.2 Terrorist Financing**

Terrorist financing refers to the accommodating or facilitating of financial transactions that may be directly or indirectly related to terrorists, terrorist activities and/or terrorist organizations. Once the financial institution knows or suspects, or should reasonably suspect that an individual/group is associated with any terrorist activity or group, a financial institution (in carrying out a transaction for or with that individual/group), may be considered to be facilitating terrorist activity whether or not the institution knows the specific nature of the activity facilitated, or whether any terrorist activity was actually carried out<sup>3</sup>.

## **4. Major AML/CFT Policy Elements for the Central Bank**

The following are the major policy elements:

- Internal controls covering all aspects of operations
- Suspicious and threshold transactions reporting
- Proper customer identification elements

---

<sup>2</sup> Taken from the BOJ AML/CFT Guidance Notes

<sup>3</sup> Taken from the BOJ AML/CFT Guidance Notes

#### 4.1 Internal Controls

##### (A) Personnel

All applicants for employment are subject to stringent due diligence background checks and depending on the nature of intended functions and the level at which they may operate in the Central Bank, they would also be subject to police checks. Thereafter personnel are required to abide by the Bank's HRA policy manual and are all required to sign to obligations of confidentiality pursuant to the Official Secrets Act before employment with the Bank commences. The manual, among other things, strictly prohibits the use of employment with the Central Bank as a means of unjust enrichment and mandates the immediate and full disclosure in any case where the duties, which the employee is required to undertake, include matters in which the employee has a personal interest. Gratuities and gifts to the employee or the family of the employee in connection with a service rendered in the employee's official capacity **are expressly forbidden**. Employees are also encouraged to immediately report any fraudulent conduct of colleagues that is suspected, noticed, or actually observed or detected.

Depending also on the nature of an employee's functions in the Central Bank, that employee is barred from, among other things, undertaking investments in the shares of deposit-taking licensees.

Promotion or the movement of employees within the Bank, must be preceded by internal due diligence within the Bank, and all employees are subject to annual performance assessments which ensure that the due diligence with regard to employees is executed on an ongoing basis.

##### (B) Operations

As regards carrying out its day-to-day activities, the Central Bank is subject to the following:

###### (1) Contract Awards Procedures

In relation to contracts to be awarded in the course of the Central Bank's maintenance and upgrading of its infrastructure - external monitoring by the National Contracts Commission in relation to contracts that reach or exceed J\$4 million (approximately US\$60,000.00 at 31 July 2006); internal monitoring of all such matters by a formally constituted Contracts Committee headed by a Deputy Governor;

(2) Financial Statement Standards and Publication Requirements

In relation to the Bank's financial statements, the Bank is subject to statutory publication requirements and in preparing these statements the Bank adheres to the IFRS rules of accounting and acts in accordance with the rules of the Institute of Chartered Accountants of Jamaica (ICAJ) on ethics;

(3) Corruption Prevention Act Statutory Declarations

Employees who earn above J\$2million (approximately US\$30,000.00 at 31 July 2006) are also subject to the statutory annual asset declaration requirements of the Corruption Prevention Act;

(4) AML/CFT Training

All employees, and particularly those assigned to the Banking Department (which directly interacts with the public), are subject to this AML/CFT policy and to the corresponding training requirements<sup>4</sup>.

**Training**

- (i) In developing training programmes<sup>5</sup>, particular emphasis is placed on the **Front Line Staff**. The first point of contact of an institution with potential money launderers or persons attempting

---

<sup>4</sup> AML/CFT training is also a special requirement for staff in the Financial Institutions Supervisory Division (FISD) and the Cambio and Remittance Units who have legal responsibility for the supervision of the country's banking and foreign exchange systems.

<sup>5</sup> See FATF Recommendation 15 and CDD Paragraphs 56 and 57 – (Taken from the BOJ AML/CFT Guidance Notes).

to finance terrorist activities is usually through staff who deal directly with the public. 'Front-line' staff members (such as Tellers, Cashiers and Foreign Currency Staff) should therefore be provided with specific training on examples of suspicious transactions and how these may be identified. To this end, guidance can be taken from the examples of transactions that would be regarded as suspicious at pages 13 - 15 of this policy. Frontline staff must also be informed about their responsibilities and the Central Bank's reporting systems and procedures to be adopted when a transaction is deemed to be suspicious. Additionally, they must be informed as to the institution's policy for dealing with occasional customers and 'one off' transactions, particularly where large cash transactions are involved.

- (ii) **Administration/Operations Supervisors and Managers** should be accorded a higher level of instruction covering all aspects of anti-money laundering procedures as these persons have the responsibility for supervising or managing staff. Such training must include familiarization with the offences and penalties arising under the MLA, the MLR, the TPA, and management's specific responsibility vis-à-vis dealings with 'high risk' transactions or business relationships.
  
- (iii) **Training therefore specifically covers:**
  - The applicable legislation - the MLA; the MLR; the BOJ's AML/CFT Guidance Notes (specifically Section II that discusses the offences of money laundering and terrorist financing, and Section III which summarizes the salient features of the MLA, MLR, and TPA); and the TPA;
  
  - FATF Recommendations, the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct



Terrorism (USA PATRIOT) Act of 2001" (the USA Patriot Act), and the Economic Sanctions Programme put in place by the USA which have extra territorial reach and which include the Foreign Narcotics Designation Kingpin Act and Regulations – (the Drug King Pin Designation Act) and the Trading With The Enemy Act. (Section III of the BOJ AML/CFT Guidance Notes also provides some guidance on this aspect of the training);

- The recognition or detection of unusual, irregular or suspicious transactions, as well as transactions which would normally be reported as Threshold Transaction Reports (TTRs)<sup>6</sup>
  - The KYC requirements for persons/institutions which interface with the Central Bank and which include:
    - Identification and Agency authorization requirements;
    - Verification of the customer's information;
    - Verification of overseas correspondent details;
    - Verification of source of funds/wealth details;
    - Purpose of transaction requirements;
  - Transactions that require senior management authorization;
  - Reporting procedures to the Central Bank's Compliance Officer;
  - The treatment of transactions deemed irregular or suspicious;
  - Conduct that might constitute "tipping off";
- (iv) Training is conducted on an on-going basis and is undertaken by a team comprising the Central Bank's legal counsel,

---

<sup>6</sup> Refers to Threshold Transaction Report form under the Money Laundering Act. Hard copies available at the Printers Office of Jamaica (26/10/2006)

AML/CFT experts from the Financial Institutions Supervisory Division and the Compliance Officer. A certificate of satisfactory completion of the employee's training in this regard should be issued at the completion of training sessions, and a record of training should be retained on the Central Bank's files.

(5) Appointment of the Compliance Officer

- (i) The Director of Banking is the assigned Compliance Officer. In his/her absence the designated compliance officer is the Assistant Director, Current Accounts.
- (ii) The "Compliance Officer" is responsible for the day-to-day monitoring of the Central Bank's compliance with this AML/CFT policy and with the AML/CFT laws, regulations and industry best practices. The Compliance Officer therefore:-
  - (a) Acts as liaison between the Central Bank and law enforcement agencies (FID, DPP, etc.) with respect to compliance matters and investigations;
  - (b) Evaluates reports of suspicious/unusual transactions and ensures the timely filing of threshold and suspicious activity reports;
  - (c) Coordinates with the Central Bank's Internal Audit, Legal and Security Departments on AML/CFT matters and investigations;
  - (d) Prepares summary (quarterly and annual) reports to the Division Chief on the effectiveness of the AML/CFT framework. These Summary Reports must also be submitted to the Bank's Management Council.

- (e) Forwards TTRs<sup>7</sup> and STRs to the Division Chief for sign off and dispatch to the Designated Authority.

STRs are required to be **promptly** reported to the Designated Authority (FID) to facilitate further investigation by that agency. The Compliance Officer is required to submit the TTRs to the Designated Authority within five (5) working days after the end of each quarter. Accordingly, the yearly reporting schedule for TTRs is as follows:

Transactions for	Report within 5 Working Days after
Jan – Mar	31 Mar
Apr – Jun	30 Jun
Jul – Sep	30 Sep
Oct – Dec	31 Dec

- (f) Along with critical input from the Bank's Senior Legal Counsels, updates policies and procedures and disseminates information to Bank personnel, as well as provides updates on pending revisions to Jamaica's AML/CFT requirements;
- (g) Oversees administrative matters related to compliance with this AML/CFT policy (including implementing compliance programmes such as appropriate record keeping requirements; development of reporting forms where necessary); and
- (h) Coordinates AML/CFT training.

<sup>7</sup> Refers to Threshold Transaction Report form under the Money Laundering Act. Hard copies available at the Printers Office of Jamaica (26/10/2006)

- (6) All operations from (1) through (5) above are also subject to audit by the Bank's Internal Audit Department whose duties include, among other things, checking to determine that Management ensures that monitoring occurs and that corrective action where necessary, is taken in a timely manner.

#### **4.2 Suspicious & Threshold Transactions Reporting (STRs and TTRs<sup>8</sup>)**

##### **(1) Suspicious Transactions**

Personnel must always be alert to situations, which may lead to money laundering and other illegal activities. The types of transactions that may be used by a money launderer are almost unlimited. However, a suspicious transaction will often be one which is inconsistent with the customer's known or legitimate business or source of funds.

Because Bank of Jamaica is not a 'deposit-taking institution', its exposure to those money laundering activities that are usually perpetrated through accounts is limited. On the other hand, it is precisely for this reason that the Central Bank must be extremely vigilant in transacting with its mainly occasional customers, as recourse thereafter may be forever lost.

- (1.1) Bank employees are required to enquire routinely about the source of funds/wealth regardless of currency. Bank personnel may be guided by Appendix I of the BOJ AML/CFT Guidance Notes which provides a guide to transactions that may be considered suspicious. However, bank personnel in particular, should be alert to:

##### Generally

- Requests for the exchange of large quantities of low denomination notes for those of higher denomination;

---

<sup>8</sup> Refers to Threshold Transaction Report form under the Money Laundering Act. Hard copies available at the Printers Office of Jamaica (26/10/2006)

- Frequent exchange of cash into other currencies;
- Purchasing of securities to be held by the financial institution in safe custody, where this does not appear appropriate given the customer's apparent standing;
- Buying and selling of a security with no discernible purpose or in circumstances which appear unusual;
- Unusual purchases or sales of foreign currency in a manner inconsistent with the customer's known foreign exchange use and requirements according to the nature of the business conducted by the customer;
- Overseas correspondent banks attempting to negotiate business with the Central Bank and which correspondents are located in jurisdictions that either do not have an existing AML/CFT regulatory regime or which have such a regime that is not on par with Jamaica's AML/CFT regulatory regime;
- Overseas correspondents seeking to conduct business from jurisdictions that are currently on FATF's list of non-cooperative countries and territories (NCCT/blacklisted territories).

#### Employee Related Transactions

- Increases in cash deposits of the staff member without apparent cause, especially if such deposits are subsequently transferred within a short period out of the account and/or to a destination not normally associated with the customer;

- Frequent exchange of cash into other currencies;
- Staff members who repay problem loans unexpectedly;
- Requests to borrow against assets where the origin of the assets is not known or the assets are inconsistent with the staff member's apparent means.

(1.2) Note that where a transaction appears to be suspicious, the transaction should not be conducted. Suspicious Transactions must be reported to the Designated Authority which is the FID<sup>9</sup>. (See Operating Procedures.) Transactions that are not at the stage of being regarded as suspicious but that appear unusual and therefore raise questions, should be flagged for closer scrutiny. If they are still conducted, they should be subjected to more intense scrutiny and should in any event be advised to the Compliance Officer and still be reported to the Designated Authority (see Operating procedures).

(2) **Threshold Transactions**

(2.1) Under the MLA, the Threshold Transaction Reports (TTR<sup>10</sup>s) must be prepared for transactions in cash (i.e. currency) exceeding the stipulated threshold of US\$50,000<sup>11</sup> or its equivalent in other currencies<sup>12</sup>. However, in light of the types of transactions that must ordinarily be undertaken by the Central Bank in relation to clearing banks or in the pursuance of its monetary policy mandate, the Central

---

<sup>9</sup> Note that since June 2003 the designated Authority was changed from the Director of Public Prosecutions (DPP) to the FID.

<sup>10</sup> Refers to Threshold Transaction Report form under the Money Laundering Act. Hard copies available at the Printers Office of Jamaica (26/10/2006)

<sup>11</sup> The new limit for threshold reporting proposed under the pending amendments to the AML framework is US\$15,000.00 and in the case of remittance companies US\$5,000.00. In the case of Cambios, the owners and managers are currently under an obligation to report transactions amounting to and exceeding US\$8,000.00

<sup>12</sup> Official transactions on behalf of the following institutions are exempt: Central Government, Statutory Bodies, Embassies and High Commissions.

Bank is not now included amongst persons that are statutorily required to report transactions of this nature. Reporting in this regard is therefore voluntary and will have regard for the particular circumstances.

- (2.2) As regards transactions conducted with Central Government, these are statutorily exempt from this requirement and the same process will be applied in relation to the Central Bank's treatment of such transactions in that a transaction report need not be generated unless the transaction is one that ought to be flagged as indicated above at paragraph (1.2) in which case the transaction should then be reported as a STR to the Designated Authority.
- (2.3) Transactions conducted with Primary Dealers, Commercial Banks and overseas correspondent banks (that operate from jurisdictions with AML/CFT regimes that meet or exceed Jamaica's regime) may be treated as transactions conducted with persons who necessarily at some point generate the levels of cash associated with the kinds of business conducted, and for which a transaction report need not be generated unless the transaction is one that ought to be flagged as indicated above at paragraph (1.2) in which case the transaction should then be reported as a STR to the Designated Authority.
- (3) Suspicious Transaction Reports (STRS) and TTRs<sup>13</sup> must be submitted to the Designated Authority (i.e. the FID). (See Operating Procedures.)

### (3.1) OPERATING PROCEDURES

Employees must take the following steps when confronted with large and/or suspicious activities:

1. Evaluate the transaction

---

<sup>13</sup> Refers to Threshold Transaction Report form under the Money Laundering Act. Hard copies available at the Printers Office of Jamaica (26/10/2006)

2. Where a transaction is considered suspicious taking into consideration the situation or the individual causing suspicion:
  - Assemble appropriate supporting transaction records.
  - Advise the Compliance Officer.
  - Prepare STR where this is authorized and dispatch immediately to the Designated Authority.
3. Any suspicious activity involving bank employees should be reported to the Deputy Governor, Banking & Market Operations Division through the Division Chief and to the Internal Auditor.
4. Where a transaction qualifies for a TTR<sup>14</sup> (US\$50, 000 or its equivalent in other currencies) prepare TTR.

#### **4.2A Transaction Limits and Source of Funds Requirements**

- (1) **For any transaction reaching or exceeding US\$1,000.00** or the equivalent amount in any other currency, notwithstanding 4.3, every person conducting business with the Bank (including Bank staff/Bank employees/and persons under contract with the Bank), **must** submit information on the source of the funds used to finance the transaction/(s) with the Bank.
- (2) Reference to income sources includes (i.e. salary; investment proceeds; gifts; sale of asset; encashment of investment portion of insurance policies or other investments; and sources of wealth (i.e. asset holdings) and so forth.
- (3) Senior Management with ultimate responsibility for banking operations within the Bank should **ensure** that the personal circumstances and income sources for persons conducting transactions reaching or exceeding US\$1,000.00 (or the

---

<sup>14</sup> Refers to Threshold Transaction Report form under the Money Laundering Act. Hard copies available at the Printers Office of Jamaica (26/10/2006)



equivalent amount in any other currency) are **known** and **verified** as much as possible.

- (4) For the avoidance of any doubt, the Bank should retain the discretion with regards to any transaction being conducted, to demand source of fund information. However, the source of funds requirement is mandatory in respect of transactions reaching or exceeding US\$1,000.00 (or the equivalent amount in any other currency).

### **4.3 Customer Identification**

Bank personnel must establish clearly the identity of each customer. At a minimum, the KYC requirements include<sup>15</sup>: -

- Processes for the identification and verification of the nature and purpose of a customer's business so that a basis is established for determining whether a transaction is unusual or suspicious, or fits the norm expected of such a business.
- Procedures for the recording and regular review of customer identification and transaction information/records to ensure that the information is current and comprehensive<sup>16</sup>, as well as the retention of such information for a minimum of five years after the transaction was initiated/attempted or had actually taken place, or the business relationship has been terminated.
- Measures to deal with special areas of operations such as high risk counterparties (eg. correspondent banks residing in countries with inadequate anti-money laundering and anti-terrorism financing measures, as well as making assessments of any person or legal entity connected with a financial transaction that could pose reputational or other risks to the Central Bank).

---

<sup>15</sup> Taken from Section IV of the BOJ AML/CFT Guidance Notes

<sup>16</sup> See also MLR Regulation 8

Where a potential customer refuses to produce the requested information, the transaction should not be completed. In addition to obtaining appropriate identification, employees are required to further ensure that the IDs are valid.

### **Identification of Natural Persons<sup>17</sup>**

The following information should be obtained from all prospective customers who do not fall in the category of employees with the Central Bank, and who do not comprise central government, a primary dealer, a commercial bank or an overseas correspondent bank:

- (a) true name and names used;
- (b) correct permanent address, including postal address;
- (c) date of birth;
- (d) nationality;
- (e) source of funds, and source of wealth, where considered appropriate;
- (f) contact numbers (work; home; cellular;)

The following are the acceptable forms of identification for individuals transacting business with the Central Bank:

- Valid Drivers licence (bearing a photograph), issued by the authority in the country in which the person is resident;
- Valid Passport;
- Valid National Identification Card

### **Identification of Corporate Bodies<sup>18</sup>**

As regards bodies corporate transacting business with the Central Bank where these persons do not fall in the category of commercial bank, primary dealer, or overseas correspondent bank, the following are required:

---

<sup>17</sup> Taken from Section IV of the BOJ AML/CFT Guidance Notes

<sup>18</sup> Taken from Section IV of the BOJ AML/CFT Guidance Notes

- (a) Certificate of Incorporation or Certificate of Registration;
- (b) Memorandum (where applicable) and Articles of Association or Partnership Deed;
- (c) Directors' Resolution authorizing company's management to engage in transactions;
- (d) Financial Institutions Mandate, signed application form, or an account opening authority containing specimen signatures;
- (e) A financial statement of the business (Audited, or in the case of companies incorporated for under eighteen months, in-house statements);
- (f) A description of the customer's principal line of business and major suppliers (if applicable);
- (g) List of names, addresses and nationalities of principal owners, directors, beneficiaries and management officers including evidence of the identity of the natural persons, that is to say, the individuals that ultimately own or control the principal;
- (h) Group/Corporate structure, where applicable.
- (i) Items (a) – (g) would not be applicable in the case of statutory bodies or government companies; however, the authorization for that company or statutory body to transact the business indicated with the Central Bank will need to be provided to the Central Bank prior to the Central Bank undertaking the transaction or commencing the business relationship.

### **Simplified KYC Procedures**

It should be noted that the FATF permits simplified or reduced CDD measures to be applied where information on the identity of the customer and the beneficial owner of the customer is publicly available, or where adequate checks and controls exist elsewhere in the system. (See FATF Recommendations 9 and 10). Examples cited by the FATF of persons in relation to whom simplified KYC/CDD measures may be applied include:

- Financial Institutions which are subject to AML/CFT requirements consistent with the FATF recommendations and which institutions are supervised for compliance with those controls.
- Public companies that are subject to regulatory disclosure requirements.
- Government administrative enterprises.

### **Central Government**

Business being transacted with the Central Government need not be subject to the usual KYC procedures, **save and except** that the Central Bank must be satisfied at all times that the person acting with the authority of the Central Government does have the authority to act in that capacity **and therefore** to conduct business with the Central Bank. To this end, complete and up-to-date notices of changes in officers acting on behalf of the Central Government should be obtained and maintained for easy retrieval as required.

**Commercial banks** are licensed under the Banking Act and regulated by the Financial Institutions Supervisory Division (FISD) of the Central Bank and are also subject to the statutory AML/CFT requirements under the MLA, the MLR, the TPA, and the BOJ AML/CFT Guidance Notes.

**Primary Dealers** are licensed under the Securities Act and as such are regulated by the Financial Services Commission (FSC). Persons licensed under the Securities Act are also subject to the statutory AML/CFT requirements under the MLA and MLR and the TPA.

Business being transacted with Commercial Banks and Primary Dealers need not be subject to the usual KYC procedures **save and except** that the Central Bank must be satisfied at all times that the person acting with the authority of the commercial bank or Primary Dealer has the authority to act in that capacity **and therefore** to conduct business with the Central Bank. To this end, complete and up-to-date notices of changes in officers acting on behalf of the commercial

banks and primary dealers should be obtained and maintained for easy retrieval as required.

## **High Risk Transactions/Business Relationships**

### **Correspondent Banking**<sup>19</sup>

Correspondent banking refers to the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Financial institutions are required by FATF to apply appropriate levels of due diligence to such accounts by gathering sufficient information from and performing enhanced due diligence processes on correspondent banks prior to setting up correspondent accounts.

- Obtaining authenticated/certified copies of Certificates of Incorporation and Articles of Association (and any other company documents to show Registration of the institution within its identified jurisdiction of residence);
- Obtaining authenticated/certified copies of banking licences or similar authorization documents, as well as any additional licences needed to deal in foreign exchange;
- Determining the supervisory authority which has oversight responsibility for the respondent bank;
- Determining the ownership of the financial institution;
- Obtaining details of respondent bank's board and management composition;
- Determining the location and major activities of the financial institution;
- Obtaining details regarding the group structure within which the respondent bank may fall, as well as any subsidiaries it may have;

---

<sup>19</sup> See FATF Recommendation 7 and CDD paragraph 49-52 – Taken from Section V of the BOJ AML/CFT Guidance Notes

- Obtaining proof of its years of operation, along with access to its audited financial statements (5 years if possible);
- Information as to its external auditors;
- Ascertaining whether the bank has established and implemented sound customer due diligence, anti-money laundering and anti-terrorism financing policies and strategies and appointed a Compliance Officer (at management level), inclusive of obtaining a copy of its AML/CFT policy and guidelines;
- Ascertaining whether the correspondent bank has, in the last 7 years (from the date of the commencement of the business relationship or negotiations therefore), been the subject of, or is currently subject to any regulatory action or any AML/CFT prosecutions or investigations. A primary source from which this information may be sought and ascertained would be the regulator for the jurisdiction in which the correspondent bank is resident. Information may also be available from its website;
- Requiring confirmation that the foreign correspondent banks do not permit their accounts to be used by shell banks;
- Establishing the purpose of the correspondent account;
- Documenting the respective responsibilities of each institution in the operation of the correspondent account;
- Identifying any third parties that may use the correspondent banking services; and
- Ensuring that the approval of senior management is obtained for the account to be opened.

While the Bank of Jamaica currently does not provide correspondent banking services to foreign banks, it does have banking relationships with overseas financial institutions and must therefore ensure that the above procedures are engaged vis-à-vis such relationships.

Additionally, the Central Bank will need to satisfy itself that the foreign respondent banks do not permit their accounts to be used by shell banks. In this regard, attention should be paid to the following indicators:

- whether the respondent bank permits “payable through accounts”. This would be one foreseeable way in which shell banks could take advantage of respondent banks;
- the country in which the foreign respondent bank resides; (see note on countries with inadequate AML/CFT frameworks). Jurisdictions with secrecy laws that prohibit the release of any KYC information or which laws present an obstacle to the KYC due diligence process.

### **Record Keeping Regarding Correspondent Banks**

Section 319(B) of the USA Patriot Act requires that financial institutions maintain records of the owners and the US agents of foreign respondent banks. Subsection (k) also authorizes the relevant authorities in the USA to issue a summons or subpoena to any foreign financial institution that maintains a correspondent account in the USA and to request records relating to such account, including records maintained outside the USA relating to the deposit of funds into the foreign bank. If a foreign bank fails to comply with or contests the summons or subpoena, any financial institution with which the foreign bank maintains a correspondent account **must** terminate the account upon receipt of notice from the authorities. Additionally, the USA Patriot Act requires foreign banks that maintain correspondent accounts with any US bank or US broker-dealer in securities to complete a certification form. This form, among other things, requires a foreign bank to certify the identity of its agent for service of legal process in the USA; that it is a supervised entity and ownership information on the foreign bank.

A foreign bank is defined as a bank organized under foreign law and located outside of the USA and includes offices, branches and agencies of commercial banks, or trust companies, private banks, national banks, thrift institutions, credit unions and other organizations chartered under banking laws and supervised by banking supervisors

of any state.<sup>20</sup> **It is noted however, that a foreign bank under that statute does not include any foreign central bank or monetary authority that functions as a central bank, or any international financial institution or regional development bank formed by treaty or international agreement.**<sup>21</sup>

### **Custody Arrangements**

Precautionary measures must be taken in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. In the unusual event that consideration is given to making such facilities available to non-account holders, there must be strict adherence to the identification procedures set out in this policy.

### **Wire Transfers And Other Electronic Funds Transfer Activities**<sup>22</sup>

The terms '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<sup>23</sup>. For all wire transfers or electronic funds transfers, whether domestic or cross border, the following information should be obtained and retained for the period stated in the MLR when conducting any/all electronic fund transfers (wire transfers, remittances etc):

- The identity of the originator/remitting customer (including name, address and account number. In the absence of an account number, a unique reference number must be included) whether or not the originator is a customer of the Central Bank; (Note that according to the interpretative note to FATF Special Recommendation 7, paragraph 2(e), the originator is an account holder, or where there is no account, the person that places the order with the financial institution to perform the wire or funds transfer);

---

<sup>20</sup> Appendix A to the rule codified at 31 CFR 103 which came into effect October 28, 2002 – OCC Bulletin OCC2002-41 issued by the Comptroller of the Currency Administrator of National Banks

<sup>21</sup> Appendix A to the rule codified at 31 CFR 103 which came into effect October 28, 2002 – OCC Bulletin OCC2002-41 issued by the Comptroller of the Currency Administrator of National Banks

<sup>22</sup> See FATF Recommendation 5 and FATF Special Recommendation on Terrorist Financing

<sup>23</sup> See the interpretative note to FATF Special Recommendation 7



- The identity of the ultimate recipient/beneficiary, where practical, including name, address and account number (in the absence of an account number, a unique reference number must be included);
- Related messages/instructions that accompany transfers.

Specifically the following should be noted:

- (i) Unless the receiving or intermediary financial institution has the technical capability to immediately access from its records, the requisite originator and beneficiary details as set out above, batch transfers should not be accepted in the course of wire transfers or any other electronic funds transfers regardless of whether such transactions qualify as 'routine' or 'non-routine' transactions.
- (ii) Transfers not accompanied by the requisite originator and beneficiary details as set out above, should not be processed by the receiving or intermediary financial institution unless and until the complete originator information is available.

### **Transferring Clients**<sup>24</sup>

Where accounts are transferred from another financial institution, enhanced KYC standards should be applied especially if there is any reason to believe that the account holder has been refused banking facilities by the other financial institution. While this is not a circumstance that may normally be encountered, staff should nonetheless be aware of the need for enhanced diligence if such were to occur.

### **Non Face-to-Face Customers**

Transactions being conducted on behalf of a beneficiary (e.g. by an employee on behalf of another employee or a walk in customer on behalf of a third party)

---

<sup>24</sup> See CDD Paragraph 29

should be subject to more rigorous verification and identification standards including independent verification by a reputable third party.

## **5 ANTI-MONEY LAUNDERING OPERATING PROCEDURES**

- 1) Threshold Transaction Report<sup>25</sup>
- 2) Suspicious Transaction Report (Attached)

Initially Prepared: March 1999

Updated: July 2006

Last Updated: November 2006

---

<sup>25</sup> Refers to Threshold Transaction Report form under the Money Laundering Act. Hard copies available at the Printers Office of Jamaica (26/10/2006)

## SUSPICIOUS TRANSACTION(S) REPORT



<b>PART 1</b>		<b>REPORTING ENTITY INFORMATION</b>
1.	Name of reporting Entity	
2.	Address of Reporting Entity	
3.	TRN of Reporting Entity	
4.	Type of Entity making this report	
<b>PART 2</b>		<b>CUSTOMER INFORMATION</b>
5.	Person/Institution/ conducting /(/who/which conducted) the transaction	First Name                      M.I.                      Last Name  <b>or</b> (ii) Insert name of company or Institution
6.	Address of the Person/Institution conducting the transaction /(/who/which conducted) the transaction	
7.	TRN of Person /Institution conducting the transaction /(/who/which conducted) the transaction	
8.	Occupation/Business/Principal Activity of the Person or Institution conducting(/who/which conducted) the transaction	
<b>TRANSACTIONS DONE ON</b>		<b>BEHALF OF CUSTOMERS</b>
10.	Name of Agent acting for customer	(i) First Name                      M.I.                      Last Name  <b>or</b> (ii) Insert name of company or other organization acting on behalf of customer
11.	Address of Agent acting for customer	
12.	TRN of Agent acting for customer	

## SUSPICIOUS TRANSACTION(S) REPORT



	<b>PART 3</b>	<b>TRANSACTION DETAILS</b>
13.	Type of Transaction conducted /being conducted	
14.	Transaction amount	
15.	Source of funds	
16.	Transaction currency &	
17.	J\$ Equivalent of the transaction amount	
	<b>PART 4</b>	<b>VERIFICATION</b>
18.	Method used to verify identity of the customer	
18A.	Indicate identification used, issuing jurisdiction, identification number and expiry date	<input type="checkbox"/> Driver's licence <input type="checkbox"/> Passport <input type="checkbox"/> National ID <div style="border: 1px solid black; height: 25px; margin-top: 5px;"></div> <div style="border: 1px solid black; height: 25px; margin-top: 5px;"></div> <div style="border: 1px solid black; height: 25px; margin-top: 5px;"></div>
19.	Method used to verify identity of the Agent	
19A.	Indicate identification used, issuing jurisdiction, identification number and expiry date	<input type="checkbox"/> Driver's licence <input type="checkbox"/> Passport <input type="checkbox"/> National ID <div style="border: 1px solid black; height: 25px; margin-top: 5px;"></div> <div style="border: 1px solid black; height: 25px; margin-top: 5px;"></div> <div style="border: 1px solid black; height: 25px; margin-top: 5px;"></div>

## SUSPICIOUS TRANSACTION(S) REPORT



	<b>PART 4 cont'd...</b>	<b>VERIFICATION</b>									
20.	Indicate verification of Authorization of person acting on behalf of customer	<input type="checkbox"/> The transaction conducted is in keeping with the permitted activity/ies outlined in the Standard Authorization from customer on file <input type="checkbox"/> Telephone check done with customer <input type="checkbox"/> Authorization from customer presented at the time the transaction was conducted and the customer signature on the authorization matches the customer's signature on file <input type="checkbox"/> Other, please specify:									
20A.	Describe verification of Customer's particulars										
20B.	Describe verification of Agent's particulars										
	<b>PART 5</b>	<b>REASON/S FOR SUSPICION</b>									
21.	Reason/(s) for Suspicion										
22.	Preparer information	<table style="width: 100%; border: none;"> <tr> <td style="width: 33%;">Last Name</td> <td style="width: 33%;">First Name</td> <td style="width: 33%;">M.I.</td> </tr> <tr> <td>Title</td> <td colspan="2">Tel. No.</td> </tr> <tr> <td>Signature:</td> <td colspan="2">Date:</td> </tr> </table>	Last Name	First Name	M.I.	Title	Tel. No.		Signature:	Date:	
Last Name	First Name	M.I.									
Title	Tel. No.										
Signature:	Date:										

Name \_\_\_\_\_  
Compliance Officer

Signature \_\_\_\_\_  
Compliance Officer

Date \_\_\_\_\_

Name \_\_\_\_\_  
Division Chief

Signature \_\_\_\_\_  
Division Chief

Date \_\_\_\_\_



## **ADDENDUM**

1. Analyze and sign off on the reports of suspicious /unusual transactions and ensures that the Compliance Officer adheres to the timely filings of threshold and suspicious activity reports to the Designated Authority.
2. Act as Liaison along with the Compliance Officer, between the Central Bank and law enforcement agencies with respect to compliance matters and investigations;
3. Review and sign off on summary (quarterly and annual) reports on the effectiveness of the Central Bank's AML/CFT framework that are submitted by Compliance Officer;
4. Ensure that the Compliance Officer updates the AML/CFT policy and procedures (inclusive of compliance programmes) from time to time to ensure continued relevance to the operations of the Central Bank;
5. Reporting to the Senior and/or Executive Management of the Bank on the AML/CFT status of the Central Bank with regards to Policy upgrades; Enhanced procedures; rate of compliance; incidence of breaches and corrective measures taken or to be taken to address the breach of the policy; systems preparedness; staff training.

**(Addendum to the Bank of Jamaica AML/CFT Policy Comprising section B(5A).**

**This addendum is to be read as one with the Bank of Jamaica AML/CFT Policy and takes effect immediately.)**

**(This Addendum also means that wherever in the Policy document the requirement is stated for the compliance officer to report to the Division Chief this should be read as the Compliance Officer is to report to the Senior Compliance Officer.)**