September 2010(revised)
July 2008 (revised)
December 2007 (revised)
November 2, 2006 (revised)
July 31, 2006 (original issue date)

BANK OF JAMAICA

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

September 2010(revised)
July 2008 (revised)
December 2007 (revised)
November 2, 2006 (revised)
July 31, 2006 (original issue date)

BANK OF JAMAICA

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

Contents — Page number/Paragraph

September 2010(revised)
July 2008 (revised)
December 2007 (revised)
November 2, 2006 (revised)
July 31, 2006 (original issue date)

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;
- Public Bodies;
- 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)
- Authorised dealers and cambios in the buying and selling of foreign currency with the Central Bank;
- Central Banks;
- Approved Overseas correspondents (i.e. foreign banks and other financial institutions approved as institutions with which the Central Bank can conduct business)
- High Commissions and Embassies;
- Multilateral agencies (including Foreign Missions);
- Employees of the Bank of Jamaica;
- Members of the public (restricted to "walk-in customers/ persons conducting one-off transactions) who:
    - Are direct holders of GOJ 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 1998

The Money Laundering Regulations, 1998

The Bank of Jamaica AML Guidance Notes 1995/(2000)

The CFATF 19 Recommendations

The FATF 40 + 8 Recommendations

The Basel Customer Due Diligence (CDD)

The applicable local legislation and international best principles have since been updated as indicated below:

- ✓ The Proceeds of Crimes Act (POCA), 2007 (This Act has repealed and replaced the Money Laundering Act, 1998 and the Regulations thereunder)

- ✓ The POCA (Money Laundering Prevention) Regulations, 2007

- ✓ The Terrorism Prevention Act, 2005

The BOJ AML/CFT Guidance Notes, 2004/(^{R}2005), (^{R}2007)[1]

The FATF 40 + 9[2] Recommendations

3. Money Laundering and Other Financial Crimes

As can be seen from the above, the profile for the Central Bank's customers 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[3]. 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;
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;

[1] Several adjustments have been effected to the Guidance Notes with the last round of revisions currently being effected to reflect the AML enhancements effected with the passage of the POCA. The draft Guidance Notes being finalized can be viewed at the BOJ's web site www.boj.org.jm

[2] The FATF 40 + 8 Recommendations were increased to FATF 40+9 Recommendations in October 2004. The ninth recommendation treats with the issue of cash couriers.

[3] The Corruption Prevention Act, 2002 requires public servants earning above a certain income bracket to file annual asset declarations with the Corruption Prevention Commission.

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[4]. Under the Proceeds of Crime Act money laundering is any activity amounting to dealings with criminal property[5]. Criminal property is any property that constitutes a benefit derived wholly or partially from criminal conduct. Criminal conduct[6] means any conduct constituting an offence in Jamaica, or if outside, conduct that would constitute a crime in Jamaica. Paragraphs 20 and 21 of the BOJ AML/CFT Guidance (Revised version August 2007)[7] briefly summarize the changes to the AML regime in Jamaica brought about with the passage of the POCA.

It should also be noted that under the POCA the successful prosecution of an offence under the AML regime does not only require proof of knowledge on the part of the person charged with the offence. It is now sufficient if it can be proven that there was wilful blindness on the part of the person so charged. That is to say, it need only be proved that in the circumstances, it would have been reasonable for the person charged to believe or know that the property being dealt with was in fact criminal property.

Employees should also note that with the passage of POCA the list of predicate offences (i.e. offences from which a money laundering charge can be derived) was significantly expanded from those contained in the schedule to the MLA (i.e. drug offences, firearms offences; any offence involving fraud, dishonesty or corruption) to any serious offence. Charges in respect of offences involving for example breaches of Intellectual Property

[4] Taken from the BOJ AML/CFT Guidance Notes
[5] See the POCA section 91(1)
[6] See the POCA section 2
[7] Several adjustments have been effected to the Guidance Notes with the last round of revisions currently being effected to reflect the AML enhancements effected with the passage of the POCA. The draft Guidance Notes being finalized can be viewed at the BOJ's web site www.boj.org.jm

rights, or breaches of the relevant financial statutes, may therefore possibly lead to additional charges of money laundering.

3.2 Criminal Lifestyle and Civil Forfeiture

The concept of criminal lifestyle and civil forfeiture were introduced by the POCA. In the case of application of the concept of criminal lifestyle, once a person has been convicted of any offence before the Supreme Court or has been committed to the Supreme Court from the RM Court pursuant to a determination on a forfeiture order or pecuniary penalty order, the Court at that point is required to make a determination on the issue of criminal lifestyle. (Section 5(1) of the POCA) (See also paragraph 107 of the BOJ AML/CFT Guidance Notes (Revised August 2007). In the case of application of civil forfeiture, law enforcement authorities may take steps to seize property believed to be obtained directly or indirectly from unlawful conduct or in connection with unlawful conduct. In these cases it is not necessary for the action of the authorities in this regard to be preceded by either a conviction or charge in relation to the property in question or the person holding the property. However the authorities must at all times act within the parameters of the statutory safeguards outlined in the POCA. (see sections 57 -71 of the POCA) (See also paragraph 107 of the BOJ AML/CFT Guidance Notes (Revised August 2007)[8]

Introduction of the civil forfeiture and criminal lifestyle regimes means that it is likely financial institutions as well as the Central Bank will need to undertake enhanced due diligence KYC measures to ensure that they are not in fact holding **forfeitable assets**[9]. This goes back to the KYC requirements at section IV of the Bank of Jamaica's AML/CFT Guidance Notes particularly those requiring financial institutions to ensure sufficient attention is paid to knowing the business of the customer /knowing the nature

[8] Several adjustments have been effected to the Guidance Notes with the last round of revisions currently being effected to reflect the AML enhancements effected with the passage of the POCA. The draft Guidance Notes being finalized can be viewed at the BOJ's web site www.boj.org.jm

[9] See POCA sections 6, s.5 (1), (2), (4), (13) & (14)

of the customer's business; and source of wealth and source of funds checks and verification.

The regimes will be subject to third party interests where genuine cases are established. Third party interests will however have to apply to the court for an order under sections 5(12) and 5(13) re: Criminal lifestyle regimes (See also section 8(3)(b); Re: Civil forfeiture see sections 58(5) 0. This means additional costs attached to protecting the institution's interest in forfeitable property that is with the institution as collateral for credit facilities extended.

The offences to which the criminal lifestyle regime applies can be found at the second schedule to the POCA (i.e drug trafficking, money laundering, murder, kidnapping, arms trafficking, forgery, infringements of intellectual property rights, larceny, embezzlement, extortion, terrorism offences and inchoate offences (conspiracy, aiding, abetting, counseling etc.).

3.3 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[10].

[10] Taken from the BOJ AML/CFT Guidance Notes - Several adjustments have been effected to the Guidance Notes with the last round of revisions currently being effected to reflect the AML enhancements effected with the passage of the POCA. The draft Guidance Notes being finalized can be viewed at the BOJ's web site www.boj.org.jm

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

The following are the major policy elements:

- Internal controls covering all aspects of operations
- Required disclosures[11] (i.e. Suspicious transactions reporting) and threshold transactions reporting[12]
- Proper customer identification elements
- Source of funds for transactions exceeding USD 1,000 or the equivalent in any other currency.

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 Human Resource (HR) 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.

[11] See the POCA section 94
[12] See the POCA (MLP) Regulations, 2007 regulation 3

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 JMD4 million (approximately USD46,000.00 at 30 September 2010; internal monitoring of all such matters by a formally constituted Contracts Committee headed by the Financial Controller

The Bank is also subject to transparency requirements to disclose to the Contractor General all contracts JMD250,000 (i.e approx. USD2,900.00 at 30 September 2010) and upwards. These disclosures must be made every month.

(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 JMD2million (approximately USD23,000.00 at 30 September 2010) 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[13]. The training in this regard becomes even more relevant now for financial institutions generally because of the revised defences that can now be raised by a person charged with an offence under the POCA. Under the POCA, not only can a person raise the defence that he or she did not know or suspect that another is engaging in money laundering, he/she can also claim that the requisite training was not provided to him or her by the employer[14]. (See the BOJ AML/CFT Guidance Notes –Revised 2009[15] – paragraphs 112 – 114)

Training

(i) In developing training programmes[16], particular emphasis is placed on the **Front Line Staff**. The first point of contact of an institution with potential money launderers or persons attempting to finance terrorist activities is usually through staff who deal

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

[14] See the POCA section 94(6)

[15] Several adjustments have been effected to the Guidance Notes with the last round of revisions currently being effected to reflect the AML enhancements effected with the passage of the POCA. The draft Guidance Notes being finalized can be viewed at the BOJ's web site www.boj.org.jm

[16] See FATF Recommendation 15 and CDD Paragraphs 56 and 57 – (Taken from the BOJ AML/CFT Guidance Notes).

directly with the public. 'Front-line' staff members (such as Tellers, Cashiers and Foreign Currency Staff possibly also security personnel and receptionists for the banking area of the Central Bank) 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 20 – 23 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 POCA, the POCA (MLP) Regulations 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 POCA; the TPA and 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 POCA and 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, required disclosure procedures (i.e. STR procedures) as well as transactions which would normally be reported as Threshold Transaction Reports (TTRs)[17]

- The KYC requirements for persons 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 Nominated Officer;

- The treatment of transactions deemed irregular or suspicious;

[17] Refer to Threshold Transaction Report form under the POCA (MLP) Regulations, 2007 Hard copies available at the Government Printing Office of Jamaica

- Conduct that might constitute "tipping off";

As regards the matter of tipping off, while the offences under the MLA were broad enough to include this activity, it should be noted that the POCA now expressly speaks to the matter. Under the POCA a tipping off offence occurs where a disclosure likely to prejudice investigations either in relation to a required disclosure or a money laundering investigation, has taken place. (See Section 97) Under the TPA a terrorism offence (akin to "tipping off") occurs where disclosure of information on actions or proposed actions of the Designated Authority relating to an investigation being conducted or about to be conducted in relation to a terrorism offence, takes place. (See section 17 of the TPA)

(iv) Training is conducted on an on-going basis and is undertaken by a team comprising the Central Bank's legal counsel, AML/CFT experts from the Financial Institutions Supervisory Division and the Nominated 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.

Compliance with this requirement to train employees is perhaps best achieved in systems which **trigger automatic training requirements on the occurrences of certain events** eg. –

- ✓ Employment;
- ✓ Promotion/lateral movement to sensitive or frontline duties;
- ✓ Expiration of minimum period since last training session which triggers refresher requirements.
- ✓ Passage of new AML/CFT legislation or amendments to existing AML/CFT legislation;

- ✓ Change in international best practice standards and requirements;
- ✓ Revision to the BOJ AML/CFT Guidance Notes
- ✓ Revision to the BOJ AML/CFT Policy

(5) Appointment of the Senior Nominated Officer ("SNO")

The Division Chief of Market Operations and Banking is the appointed SNO[18] and this function entails the following-

a. Analyze and sign off on the reports comprising required disclosures (i.e. suspicious /unusual transactions) and ensures that the Nominated Officer adheres to the timely filings of threshold and required disclosures to the Designated Authority.

b. Act as liaison along with the Nominated Officer, between the Central Bank and law enforcement agencies with respect to compliance matters and investigations;

c. 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 the Nominated Officer;

d. Ensure that the Nominated 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;

e. 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; level of compliance; incidence of breaches and corrective measures taken or to be taken to address the breach of the policy; systems preparedness; staff training.

(6) Appointment of the Nominated Officer

(i) The Head of the Banking Department is the assigned Nominated Officer. In his/her absence the designated nominated officer is the Head, Current Accounts Section

[18] This appointment was effective 11 October, 2006

(ii) The "Nominated 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 Nominated 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 Protective Services Departments on AML/CFT matters and investigations;

(d) Prepares summary (quarterly and annual) reports to the Senior Nominated Officer on the effectiveness of the AML/CFT framework. These Summary Reports must also be submitted to the Bank's Management Council.

(e) Forwards TTRs[19] and Required disclosures (i.e. STRs) to the Senior Nominated Officer for sign off and dispatch to the Designated Authority.

Required disclosures (i.e. STRs) are required to be **promptly** reported to the Designated Authority (FID) to facilitate further investigation by that agency. The Nominated Officer is

[19] Refer to Threshold Transaction Report form under the POCA (MLP) Regulations, 2007. Hard copies available at the Printers Office of Jamaica

required to submit the TTRs to the Designated Authority within five (5) business days after the end of each quarter. Accordingly, the yearly reporting schedule for TTRs is as follows:

Transactions for	Report within 5 Business 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.

(7) 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 Required Disclosures (i.e. Suspicious Activity Reporting) & Threshold Transactions Reporting (SARs and TTRs[20])

(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:

(1.1. a) Generally

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

- Frequent exchange of cash into other currencies;

[20] Refers to Threshold Transaction Report form under the POCA (MLP) Regulations, 2007. Hard copies available at the Printers Office of Jamaica

- Frequent buying and selling of currency by any medium (cash, cheques; electronic purse or other telephonic or electronic medium etc.) in any manner that is indicative of foreign exchange trading and the transaction is not done by or on the behalf of a cambio/bureau de change or authorized dealer;

- 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;

- 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;

- Transactions constituting the co-mingling of company funds with an individual's account or constituting the conduct of company business through the account of an individual particularly where the individual is not named as a signatory to the corporate bank account.

- 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 and other foreign counterparts[21] seeking to conduct business from jurisdictions that are currently on FATF's list of non-cooperative countries and territories (NCCT/blacklisted territories).

- Overseas correspondents and other foreign counterparts[22] with principals that are included on the U.N.'s list of terrorists and seeking to conduct business directly or indirectly through a separate corporate vehicle (eg. special purpose vehicle (s.p.v.); or trustee; etc.)

- Joint venture-type invitations from local or overseas companies or organizations with no discernible track record of legitimate operations; tax compliance; and in respect of which the true identities and sources of funding or wealth of the principal/(s) are unknown.

- Purposeless conversation requesting detailed disclosures of AML/CFT measures in respect of physical location measures and software and administrative measures.

- Transactions which are started and then abandoned due to decision not to proceed or because an error was made in processing the transaction. Such incidences should be carefully monitored and care should be taken to ensure completed and/or signed documentation in this regard are properly destroyed (i.e. shredded, or finely torn/cut up) in the presence of the signing parties.

- Pre-prepared transaction forms and pre-prepared authorizations should be routinely reviewed for relevance and updated accordingly. Obsolete forms and authorizations should be meticulously destroyed

[21] See paragraph 2.1 above
[22] See paragraph 2.1 above

and every effort to ensure the proper notification of the revised form and uselessness of obsolete forms should be given to the relevant stakeholders (i.e. customers; counterparts; management and staff).

(1.1(b)) 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.

- Refusal to comply with disclosure and other AML/CFT requirements that amount to standard requirements for the operation of an account with the Central Bank.

(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[23]. (See Operating Procedures.) Transactions that are not at the stage of being regarded as suspicious but that appear unusual and

[23] Note that since June 2003 the designated Authority was changed from the Director of Public Prosecutions (DPP) to the FID.

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 Nominated Officer and still be reported to the Designated Authority (see Operating procedures).

(1.3) **The Required Disclosure Regime under POCA**

Paragraph 20.3 of the BOJ AML/CFT Guidance Notes (Revised 2009) outline the regime which –

- Imposes a 30 day reporting period on required disclosures (STRs) i.e. 15 days to report an incident to the nominated officer from the time the matter comes to a person's attention and 15 days for the nominated officer to make the required disclosure to the designated authority.

- Stipulates that the information or matters on which a person's knowledge or belief is based should have come to that person in the course of a business in the regulated sector;

- Extends the duty to report beyond transactions being conducted with customers to transactions that another person has engaged in that could constitute or be related to money laundering;

- Includes a statutory reporting form under the POCA (MLP) Regulations, 2007 to facilitate the required disclosures filing – (See Form 1 of the Schedule to these Regulations).

In keeping with the practice of aligning the AML/CFT Policy with statutory AML/CFT requirements applicable to financial institutions, the Central Bank will be adhering to the statutory reporting timeframes.

How should suspicious situations be handled – Paragraphs 20.3.5 and 20.3.6 of the BOJ AML/CFT Guidance Notes (Revised August 2007) seek to provide some guidance in this regard. The Guidance Notes therefore:-

(a) Speak to refusing to conduct the transaction or refusing to commence the relationship or declining the undertaking of any business arrangements in respect of the customer or transaction or arrangement that is deemed suspicious and in respect of which it would be reasonable to make a required disclosure (STR)

(b) Point out that if the institution is placed in a position where it is of the view that it must proceed with the transaction, relationship or arrangement, then the institution **must** ensure that the relevant disclosure has been made **and** appropriate consent to proceed is in place (see section 93(2); 99(1) & (2) and 100(4) &(5) of the POCA)

(c) Point out that if the institution is placed in a position where it is of the view that it must proceed with the transaction, relationship or arrangement, **and** in the institution's view the circumstances do not permit the institution to make the relevant disclosure **and** secure the appropriate consent **before** proceeding **then the institution must ensure** that the relevant disclosure is made **on its own initiative** and **as soon as is reasonably practical** for this to be done. (see section 93(2); 99(1&2) and 100(4) &(5)) of the POCA)

(d) Caution financial institutions to satisfy themselves that the direction or consent obtained from the designated authority **clearly permits or prohibits** the doing or undertaking of any activity in relation to accounts, transactions, customers or property in respect of which authorized disclosures have been made.

Some of the Offences under the required disclosure regime under the POCA

Section 92(2) of the POCA creates an offence where a person enters into or becomes involved in an arrangement that facilitates the acquisition, retention, use or control of criminal property by or on behalf of another **(s. 92(2)**. It therefore means the offer of any kind or type of service eg. custodian or asset safe keeping purposes provided for property that is criminal property, or even possibly issuing letters of credit on behalf of persons who proceed to use these arrangements to acquire property constituting criminal property can expose the Central Bank to liability under this section of the POCA. The penalty on conviction in the case of an individual is a fine not exceeding $3million and/or imprisonment for a term nit exceeding five (5) years, in the case of a body corporate, a fine not exceeding $5million.

Section 93 (1) of the POCA makes it an offence where a person acquires, uses or has possession of criminal property and the person knows or has reasonable grounds to believe that the property is criminal property. The penalty on conviction in the case of an individual is a fine not exceeding $3million and/or imprisonment for a term not exceeding five (5) years, in the case of a body corporate, a fine not exceeding $5million.

Section 94(2) Failing to make the requisite disclosure within the stipulated timeframe in circumstances where there is knowledge or belief that another person has engaged in a transaction that could constitute or be related to money laundering, and this knowledge or belief arose in the course of a business in the regulated sector;(STR obligation) The penalty on conviction before a Resident Magistrate is a fine not exceeding $1million and/or imprisonment for a term not exceeding 12 months. The penalty on conviction before the Circuit Court is a fine and/or imprisonment for a term not exceeding 10 years.

Section 95 - Failure of the nominated officer to make the requisite disclosure within the stipulated timeframe (i.e. within 15 days after the information or matter comes to the nominated officer's attention) in circumstances where there is knowledge or belief on the part of the nominated officer that another person has engaged in a transaction that could constitute or be related to money laundering, and this knowledge or belief arose in the course of a business in the regulated sector. (STR obligation) The penalty on conviction before a Resident Magistrate is a fine not exceeding $1million and/or imprisonment for a term not exceeding 12 months. The penalty on conviction before the Circuit Court is a fine and/or imprisonment for a term not exceeding 10 years.

Suspicious activity reports (which include transactions considered suspicious) should be made in writing to the designated authority pursuant to section 100 of the POCA (see Sample letter attached at the back of this Policy). The POCA does not have a statutory reporting form for reports made pursuant to section 100, it is however best if these reports contain all the information that is required on the statutory STR form, and such reports should be accompanied by any supporting documentation pertinent to the report.

(2) **Threshold Transactions**

(2.1) Under the POCA (MLP) Regulations, 2007 (r. 3(1)), the Threshold Transaction Reports (TTR[24]s) must be prepared for transactions in cash (i.e. currency) exceeding the stipulated threshold of USD15,000[25] or its equivalent in other currencies[26]. However, in light of the types of transactions that must ordinarily be undertaken by the Central Bank

[24] Refers to Threshold Transaction Report form under the POCA (MLP) Regulations, 2007 Hard copies available at the Government Printing Office of Jamaica

[25] Under the POCA (MLP) Regulations, 2007 (r. 3(8) the new limit for threshold reporting in the case of remittance companies US$5,000.00. In the case of Cambios, reporting obligation in this regard remains at transactions amounting to and exceeding US$8,000.00. The revised reporting limits became effective on July 1, 2007.

[26] Official transactions on behalf of the following institutions are exempt: Central Government, Statutory Bodies, Embassies and High Commissions.

in relation to clearing banks or in the pursuance of its monetary policy mandate, the Central 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 be deemed "suspicious" and reported to the Designated Authority pursuant to the "authorized disclosure provision of the POCA (i.e. section 100).

(2.3) Transactions conducted with Primary Dealers, Commercial Banks, Cambios 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 be deemed "suspicious" and reported to the Designated Authority pursuant to the "authorized disclosure" provision of the POCA (i.e. section 100).

(2.4) Authorized disclosures and TTRs[27] must be submitted to the Designated Authority (i.e. the FID). (See Operating Procedures.)

[27] Refer to Threshold Transaction Report form under the POCA (MLP) Regulations, 2007. Hard copies available at the Printers Office of Jamaica

(3) OPERATING PROCEDURES

(3.1 (a)) Maintenance of Customer Service

It is important that in enforcing the requirements of this policy that bank staff at all times operate in a professional manner. This means –

a. The consistent application of the requirements at all times regardless of the person involved in the transaction at hand;

b. Taking the steps necessary to ensure that prior advisories are issued to persons conducting transactions with the bank of any changes in transaction requirements to minimize any inconvenience to those persons.

c. Speaking with, or to persons and not "at them" whilst conducting the transaction at hand or whilst dealing with enquiries. Routine questions posed to bank staff should be taken as an opportunity to refresh one self of the AML/CFT and other operational, administrative requirements associated with banking transactions as against seeing such routine queries as the customer or other person "being a bother" or "making life hard" or deliberately "being an annoyance". It is also important that in posing routine transaction requirements to customers or other persons, that the banking staff member does not come across as "being inquisitive". At all times the point should be firmly and politely made that these are standard AML/CFT operating requirements.

d. Harsh words or aggression from customers or persons conducting transactions with the Central Bank should not be met with like responses. Difficult customers or counterparties should be quickly

referred to senior floor managers who should be able to diffuse the situation as against exacerbating the situation.

It should be noted that the foregoing AML/CFT requirements are not meant to transform banking staff into "the police", as such the foregoing should not be interpreted as a licence to intimidate persons conducting transactions with the bank or to "spy" on such persons. The foregoing is also not meant for employees to place themselves in harm's way. The foregoing merely requires vigilance in ensuring that transactions undertaken are genuine, and do not appear to be furthering or facilitating a financial crime, be it fraud, theft, or otherwise.

(3.1(b)) **Applicability of the BOJ Human Resource (HR) Policy Manual**

Threats of any kind to the personal safety of bank staff should be immediately reported to the senior floor manager and the Nominated and Senior Nominated Officer and/or (where applicable) reported in accordance with the procedures outlined in the Central Bank's HR Policy Manual. It should be noted that the conduct of employees of the Central Bank should be at all times in accordance with the requirements of the HR Policy Manual. Accordingly where in the course of the foregoing any departures in this regard take place, the process of addressing such departures will be informed by the applicable processes outlined in the HR Manual and with any other determinations made by the Central Bank.

(3.1 (c)) **Practical Operational Enforcement**

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

1. Evaluate the transaction

2. Where a transaction is considered suspicious taking into consideration the situation or the individual causing suspicion:
   - Assemble appropriate supporting transaction records.
   - Advise the Nominated 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[28] (USD15,000 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 USD1,000.00 (or the equivalent amount in any other currency) are **known** and **verified** as much as possible.

[28] Refer to Threshold Transaction Report form under the POCA (MLP) Regulations, 2007 . Hard copies available at the Printers Office of

(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 USD1,000.00 (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[29]: -

- 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[30], 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

[29] Taken from Section IV of the BOJ AML/CFT Guidance Notes - Several adjustments have been effected to the Guidance Notes with the last round of revisions currently being effected to reflect the AML enhancements effected with the passage of the POCA. The draft Guidance Notes being finalized can be viewed at the BOJ's web site www.boj.org.jm

[30] See also regulation 7 the POCA (MLP) Regulations, 2007

with a financial transaction that could pose reputational or other risks to the Central Bank).

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.

(4.3.1) **Identification of Natural Persons**[31]

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, cambio or an approved 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;)

(g) Taxpayer Registration Number (TRN)[32]*

[31] Taken from Section IV of the BOJ AML/CFT Guidance Notes - Several adjustments have been effected to the Guidance Notes with the last round of revisions currently being effected to reflect the AML enhancements effected with the passage of the POCA. The draft Guidance Notes being finalized can be viewed at the BOJ's web site www.boj.org.jm

[32] The Bank has advised the financial sector that under the POCA (MLP) Regulations, customer information includes the TRN or other reference number (in the circumstances this may include NIS or other official number issued by a Government department) Unique reference numbers generated by the financial institution may be applicable however before proceeding, the financial institution always has to be cognizant of what its legal position will be if it should be served with a customer information order pursuant to section 120 of the POCA.

* As regards the inclusion of the TRN requirement in the KYC details, the following should be noted-

i. Under the POCA (MLP) Regulations, 2007, "customer information" is now defined in regulation 7 which states that this "includes the applicant for business's full name, current address, **taxpayer registration number** or other reference number date and place of birth (in the case of a natural person) and, where applicable, the information referred to at regulation 13(c) (i.e. identity of beneficial owner).

ii. Under section 120 of the POCA, customer information also refers to the customer's TRN which forms a part of the information an institution must present/produce in compliance with a customer information order. For more on the customer information order see paragraph 107(F) of the BOJ AML/CFT Guidance Notes (Revised 2009).

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

(4.3.2) Identification of Corporate Bodies[33]

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 approved overseas correspondent bank, the following are required:

(a) Certificate of Incorporation or Certificate of Registration;

(b) Articles of Incorporation[34] 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) A copy of the licence/approval to operate where the principal line of business is one that falls under a regulatory/supervisory body.

(h) 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;

(i) Group/Corporate structure, where applicable;

(j) Items (a) – (i) would not be applicable in the case of statutory bodies or government companies; however, the authorization for that company or

[33] Taken from Section IV of the BOJ AML/CFT Guidance Notes - Several adjustments have been effected to the Guidance Notes with the last round of revisions currently being effected to reflect the AML enhancements effected with the passage of the POCA. The draft Guidance Notes being finalized can be viewed at the BOJ's web site www.boj.org.jm

[34] Under the new Companies Act, 2004 the requirement of Memorandum of Association has been discontinued, however, Memorandum and Articles of Association would still be relevant for the purpose of these Guidance Notes until these documentation have been updated pursuant to the new Companies Act.

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

(k) Tax Compliance Certificate

(4.3.3) **Enhanced KYC requirements under the POCA (MLP) Regulations, 2007**

The enhanced KYC requirements under the POCA (MLP) Regulations, 2007 are:-

(a) The establishment of statutory minimum KYC requirements by virtue of regulation 7 which contains the following definition of "customer information - "Customer information includes applicant for business's full name, current address, taxpayer registration number or other reference number, date and place of birth (in the case of a natural person) and, where applicable, the information referred to in regulation 13(1)(c);"

(**See also section 122(1) of the POCA which outlines the KYC information a financial institution must be in a position to provide pursuant to** customer information orders.

(b) In addition to this the POCA (MLP) Regulations, 2007 requires the following-

1) Periodic updates of customer information must be carried out at least once every five years; (R. 7(1)(c) & (d)) This requirement extends to the existing client base of financial institutions; (R. 19)

2) Transaction verification procedures must be applied particularly in the circumstances specified in regulation 7(3) which include – cases where the transaction meets the TTR limit 7(5); wire transfer transactions; the situation is one requiring a STR to be made; where there is doubt about the accuracy of any previously obtained evidence of identity;

3) KYC details must be retained for electronic funds transfers; (R. 9)

4) Procedures must be in place to ensure that the identities of both principals and agents are obtained in the case of transactions being conducted by a person on behalf of another; (r. 11, 12 and 13)

5) Retention of records not only for identification records, but also for transaction records; (R. 14)

6) Financial institutions must adhere to the prohibition against maintaining anonymous, fictitious accounts or numbered accounts; (R. 16)

KYC for members of the public (restricted to "walk-in customers/ persons conducting one-off transactions)[35]

Walk-in-customers or persons conducting "one-off" transactions with the BOJ may also be repeat customers. The applicable identification requirements for these persons are those outlined for natural persons and corporate bodies (whichever is appropriate) at 4.3 above. These persons are also subject to the source of funds requirements in respect of transactions amounting to, or exceeding USD1,000.00 (or the equivalent in any other currency).

However, considering the customer profile of these persons, it might not in all cases be practicable or feasible for the normal KYC verification process pertaining to source of funds to be fully applicable to clients conducting the following transaction/(s):-

- changing out of coins for notes and vice versa;
- surrendering notes and coins that are no longer in circulation;
- replacing torn or mutilated notes for new notes;

For amounts reaching or exceeding USD 1,000.00 (or the equivalent in any other currency), persons must provide evidence of the source of funds. Where,

[35] See paragraph 2.1 above

however, this cannot be substantiated, a letter signed by a Justice of the Peace, Notary Public, School Principal or Minister of Religion (Licensed Marriage Officer) w**ho knows of the business or circumstances of the funds** must be presented. The Bank reserves full discretion in these circumstances as to whether additional requirements will be imposed to facilitate its verification of the source of funds, or whether the transaction will be declined.

(4.3.4.) **Simplified KYC Procedures**

It should be noted that the FATF permits simplified or reduced Customer Due Diligence (CDD) measures to be applied where information on the identity of the customer and where the customer is a body corporate, 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.

FATF also permits the application of the de minimis transaction concept in respect of certain transactions.

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 POCA, the POCA (MLP), 2007, the TPA, and the BOJ AML/CFT Guidance Notes[36].

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 POCA, the POCA (MLP), 2007 the TPA and the FSC AML/CFT Guidelines.

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.

It should also be noted that the POCA (MLP) Regulations, 2007 has statutorily established the concept of de minimis transactions. Under this concept certain identification procedures will not be required in respect of transactions below US$250.00 unless the nature of the transaction is suspicious. The concept is not applicable to remittance transactions. The

[36] Several adjustments have been effected to the Guidance Notes with the last round of revisions currently being effected to reflect the AML enhancements effected with the passage of the POCA. The draft Guidance Notes being finalized can be viewed at the BOJ's web site www.boj.org.jm

BOJ AML/CFT Guidance Notes (Revised 2009)[37] contains a new section treating with this issue (i.e. Section IVA. 1) In keeping with the practice of aligning the AML/CFT Policy with statutory AML/CFT requirements applicable to financial institutions, the Central Bank will be adhering to the de minimis concept now statutorily permitted by POCA.

(4.3.5) **High Risk Transactions / Business Relationships**

Correspondent Banking [38]

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 Incorporation[39] (and any other company documents to show Registration of the institution within its identified jurisdiction of residence);

[37] Several adjustments have been effected to the Guidance Notes with the last round of revisions currently being effected to reflect the AML enhancements effected with the passage of the POCA. The draft Guidance Notes being finalized can be viewed at the BOJ's web site www.boj.org.jm

[38] See FATF Recommendation 7 and CDD paragraph 49-52 – Taken from Section V of the BOJ AML/CFT Guidance Notes

[39] Under the new Companies Act, 2004 the requirement of Memorandum of Association has been discontinued, the new documentation applicable is "Articles of Incorporation. However, the Memorandum and Articles of Association would still be relevant for the purpose of these Guidance Notes until these documentation have been updated pursuant to the new Companies Act.

- 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;
- 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. If the Bank of Jamaica was required to provide correspondent banking services to foreign counterparts the requirements would include the matters outlined above and may also include considerations such as -

SWIFT membership;
Licence to undertake banking and/or securities business;
Stock Exchange listing in G10 country or in approved CARICOM State.

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.[40] **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.**[41]

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

[40] See 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

[41] See 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

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[42]

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[43]. 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);
- 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:

[42] See FATF Recommendation 5 and FATF Special Recommendation on Terrorist Financing

[43] See the interpretative note to FATF Special Recommendation 7

(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.

It should be noted that the **Electronic Transactions Act, 2006** has been in effect since April 2007. In conducting transactions that fall within the parameters of this Act the provisions of this Act particularly those treating with the issue of electronic signatures (See section 8[44] "Requirements for signature") should be borne in mind.

---

[44] 8. Requirements for signature.

"8.-(1) A law requiring a person's signature in relation to any information shall be taken to have been met where the information is given electronically and-

(a) a method is used to identify the person and to show the person's approval of the information given;

(b) having regard to all the relevant circumstances when that method was used, including any relevant agreement, the method was as reliable as was appropriate for the purposes for which the information was communicated;

(c) if the signature is required to be given to the Government and the Government requires that the method used be in accordance with particular information technology requirements, the Government's requirement has been met; and

(d) if the signature is required to be given to a person other than the Government, that person consents to that requirement being met by using the method mentioned in paragraph (a).

(2) Subject to subsection (3), an encrypted signature shall be presumed to have satisfied the requirements of subsection (1) (a) and (b) if that signature is-

(a) uniquely linked to the person whose signature is required;

(b) capable of identifying that person;

Transferring Clients[45]

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.

(c) created by using means that such person can maintain under his sole control; and

(d) linked to the information to which it relates in such a manner that any subsequent alteration of the information is revealed.

(3) Subsection (2) shall not be construed as limiting in any way the ability of any person to-

(a) establish in any other manner, for the purpose of satisfying the requirement referred to in subsection (1), the reliability of an encrypted signature or other method of indicating identity and approval;

(b) adduce evidence of the unreliability of an encrypted signature.

(4) Subsection (1) applies whether the requirement for a signature is in the form of an obligation or the law merely provides consequences for the absence of a signature.

(5) In determining whether, or to what extent, a certificate or an encrypted signature is legally effective, no regard shall be had to the geographic location

(a) where the certificate is issued or the encrypted signature is created or used; or

(b) of the place of business of the certification service provider or signatory.

(6) This section shall not affect the operation of any other law that requires

(a) information that is given electronically to contain an encrypted signature (however described);

(b) information that is given electronically to contain a unique identification in an electronic form; or

(c) a particular method to be used for information that is given electronically to identify the originator and to show that the originator approved the information given."

[45] See CDD Paragraph 29

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

5 ANTI-MONEY LAUNDERING/COUNTER TERRORIST FINANCING REPORTING

1) Threshold Transaction Reporting[46]
2) Section 100 Reports (Authorized Disclosures of suspicious activities (including suspicious transactions)[47] (Sample letter attached)

[46] In keeping with the past practice of aligning the AML/CFT Policy with statutory requirements applicable to financial institutions the BOJ will be issuing such reports in a form structured to capture the information that would be required in the statutory TTR form applicable to the regulated financial sector under the POCA (MLP) Regulations, 2007.

[47] In keeping with the past practice of aligning the AML/CFT Policy with statutory requirements applicable to financial institutions the BOJ will be issuing such reports in letter form but structured to capture the information that would be required in the statutory STR form applicable to the regulated financial sector under the POCA (MLP) Regulations, 2007. The BOJ's reporting of suspicious transactions is undertaken pursuant to section 100 of the POCA.

September 2010(revised)
July 2008 (revised)
December 2007 (revised)
November 2, 2006 (revised)
July 31, 2006 (original issue date)

SAMPLE LETTER

The Chief Technical Director

Financial Investigations Division

Ministry of Finance and the Public Service

Shalimar Avenue

Kingston

Dear Chief Technical Director,

Report generated pursuant to section 100 of the Proceeds of Crime Act

We write pursuant to section 100 of the Proceeds of Crime Act in relation to the matters and persons described below.

On the day of , Mr./Ms. Mrs. (first and last names)_____ /_____Ltd. (full company or business name) of _____(given address) _____conducted transaction/(s) /attempted to conduct transaction/(s) involving the_____

_____

_____

_____.

The transaction value totaled J$/USD/Cdn./Euro/Sterling_____

Transaction details_____

_____

_____

TRN_____

ID tendered_____

ID Particulars_____

Source of funds indicated_____

Reason or basis for suspicion_____

Accounts/(s) affected (if any)_____

Person on whose behalf the transaction was being conducted (full names and address)_

The transaction was

a) not conducted;
b) conducted and the disclosure is now being made pursuant to section 101(5)(i) of the POCA;
c) conducted and the disclosure is now being made pursuant to section 101(5)(ii) of the POCA;
d) conducted and the disclosure is now being made pursuant to section 101(5)(iii) of the POCA;

The following documents are also attached/enclosed for your attention

(a)
(b)
(c)

The matter is now referred for your urgent attention.

Yours sincerely,

Senior Compliance Officer/
Compliance Officer

Att./Enc./

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 bye 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.)