BANK OF JAMAICA

MEETING OF THE BOARD OF DIRECTORS

23 JUNE 2021

BANK OF JAMAICA AML/CFT/CFP POLICY

BANK OF JAMAICA POLICY ON COMBATTING MONEY LAUNDERING (AML), AND THE FINANCING OF TERRORISM (CFT) AND PROLIFERATION OF WEAPONS OF MASS DESTRUCTION (CFP)
# TABLE OF CONTENTS

**FOREWORD** ........................................................................................................................................... v

**GLOSSARY** ........................................................................................................................................... vi

**ACRONYMS** ........................................................................................................................................... vii

1. **OBJECTIVE** .......................................................................................................................................... 1

2. **CONTEXT AND BACKGROUND** ....................................................................................................... 1

   2.1. Central Bank Objectives and Functions ......................................................................................... 2

3. **CUSTOMERS OF THE CENTRAL BANK** .......................................................................................... 2

4. **LEGISLATIVE FRAMEWORK AND SYSTEMS** .................................................................................. 4

5. **RISK BASED FRAMEWORK** ............................................................................................................. 6

6. **RISK ASSESSMENT GUIDE** .............................................................................................................. 8

7. **MAJOR AML/CFT/CFP POLICY ELEMENTS FOR THE CENTRAL BANK** ...................................... 11

   7.1. Internal Controls Covering all Aspects of Operations ....................................................................... 11

   7.1.1. Fit and Proper Checks ................................................................................................................. 12

   7.1.2. Anti-Bribery and Corruption Prevention ..................................................................................... 13

   7.1.3. Post-Employment Conditions ..................................................................................................... 14

   7.1.4. Adherence to Policies and Procedures ....................................................................................... 15

   7.1.5. Annual Training Requirements for Critical Persons - AML/CFT/CFP Training ......................... 16

   7.1.6. Training for the Executive Management and Board of the Central Bank ................................. 21

   7.1.7. Records Retention Policy ........................................................................................................... 22

   7.1.8. Cybersecurity ............................................................................................................................. 22

   7.1.9 Relationship with Audit, Risk and Compliance Functions ........................................................... 22

   7.1.10 The Senior Nominated Officer and the Nominated Officer .................................................... 23

   7.2. Required Disclosures ....................................................................................................................... 25

   7.2.1. Reports to the Designated Authority ............................................................................................. 25

   7.2.1.1 Threshold Transactions ............................................................................................................ 25

   7.2.1.2 Suspicious Transactions .......................................................................................................... 27

   7.2.2. The Required Disclosure Regime under POCA ......................................................................... 29

   7.2.3. The Reporting Regimes under the TPA ...................................................................................... 30


   7.3. KYC and CDD ................................................................................................................................... 32
| Appendix II | FATCA | 67 |
| Appendix III | Applicable Extracts from the Human Resource (HR) Policy Manual | 69 |
| Appendix IV | The Proceeds of Crime (Money Laundering Prevention) Regulations Schedule - Form I | 71 |
| Appendix V | Examples of Unusual/Suspicious Activities | 74 |
| Appendix VI | Some of the Offences under the Required Disclosure Regime Under the POCA | 79 |
| Appendix VII | Some of the Financing of Terrorism Offences under the TPA | 81 |
| Appendix VIII | Section 8 of the Electronic Transactions Act | 84 |
FOREWORD

This Policy is periodically revised and updated to take account of amendments to the AML/CFT/CFP laws and framework in Jamaica, as well as guidelines issued from time to time by the FATF/CFATF. The revision history of this policy is set out below;

March 2021 (revised)
September 2010 (revised)
July 2008 (revised)
December 2007 (revised)
November 2, 2006 (revised)
July 31, 2006 (original issue date)
### GLOSSARY

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Board”</td>
<td>means the Board of the Bank of Jamaica as established under Section 6 of the Bank of Jamaica Act;</td>
</tr>
<tr>
<td>“Designated Authority”</td>
<td>means the Financial Investigations Division (&quot;FID&quot;);</td>
</tr>
<tr>
<td>“Management Committee”</td>
<td>means the body within Bank of Jamaica that comprises the Senior Executives who have been appointed Deputy Governors under The Bank of Jamaica Act and which body is chaired by the Governor of the Bank;</td>
</tr>
<tr>
<td>“Politically Exposed Persons”</td>
<td>means an individual who meets the description of a person described at Regulation 7A (6) of The Proceeds of Crime (Money Laundering Prevention) Regulations, 2007 (amended 2013) and regulations 6A (6) of The Terrorism Prevention (Reporting Entities) Regulations, 2010 (amended 2013);</td>
</tr>
<tr>
<td>“Shell Bank”</td>
<td>has the meaning assigned in the Banking Services Act.</td>
</tr>
<tr>
<td>ACRONYMS</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------</td>
</tr>
<tr>
<td>AML/CFT/CFP</td>
<td>Anti-Money Laundering/Combatting the Financing of Terrorism/Combatting the Financing of the Proliferation of Weapons of Mass Destruction</td>
</tr>
<tr>
<td>CFATF</td>
<td>Caribbean Financial Action Task Force</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FI</td>
<td>Financial Institution</td>
</tr>
<tr>
<td>FSRB</td>
<td>FATF Styled Regional Body</td>
</tr>
<tr>
<td>GOJ</td>
<td>Government of Jamaica</td>
</tr>
<tr>
<td>IGA</td>
<td>Intergovernmental Agreement</td>
</tr>
<tr>
<td>POCA</td>
<td>The Proceeds of Crime Act</td>
</tr>
<tr>
<td>POC (ML) Regulations</td>
<td>The Proceeds of Crime (Money Laundering Prevention) Regulations</td>
</tr>
<tr>
<td>TPA</td>
<td>The Terrorism Prevention Act</td>
</tr>
<tr>
<td>TP Regulations</td>
<td>The Terrorism Prevention (Reporting Entities) Regulations</td>
</tr>
<tr>
<td>UNSCRIA Regulations</td>
<td>The United Nations Security Council Resolution Implementation Act</td>
</tr>
<tr>
<td>UNSCRIA Regulations</td>
<td>The United Nations Security Council Resolution Implementation (Reporting Entities) Regulations</td>
</tr>
</tbody>
</table>
1. OBJECTIVE
The key objective of Bank of Jamaica’s AML/CFT/CFP Policy is to provide a framework to assist the Central Bank with ensuring that its services and facilities are not used in the commission of, or to further the commission of money laundering or financing of terrorist activities or financing of the proliferation of weapons of mass destruction. The policy is also intended to ensure that, in so far as targeted financial sanction directives of the United Nations may apply to a transaction to be conducted with, or assets held by, a customer of the Central Bank, that the directive to the sanction is obeyed.

This policy therefore establishes for the management and employees of the Central Bank, guidance and rules as regards their expected roles and conduct that are required to ensure adherence to their respective AML/CFT/CFP obligations and the AML/CFT/CFP procedures that have been, and which will continue to be implemented by the Bank.

While not included in the definition of ‘financial institution’ outlined in Jamaica’s AML/CFT/CFP legislation, the Central Bank is committed to employing and applying policies in keeping with the national and international AML/CFT/CFP requirements and applicable standards. Accordingly, the policy addresses matters such as reporting to the Designated Authority on “Threshold Transactions” and “Suspicious Activities” and other nuances related to the Central Bank’s Nominated Officer regime.

2. CONTEXT AND BACKGROUND
This policy has been prepared against the background of the functions and statutory objectives of the Central Bank, and also with regard to the customer profile and by extension the AML/CFT/CFP risks to which the Central Bank may be subject, by virtue of its operations and the persons/institutions with which it conducts business.
2.1. Central Bank Objectives and Functions

In December 2020, amendments to the Bank of Jamaica Act were passed and these amendments, among other things, clarify the principal objectives of the Central Bank as being:

a. the maintenance of price stability and

b. financial system stability,

with the primary objective being the maintenance of price stability.

Other amendments effected to the Act serve to strengthen the Central Bank’s governance framework to ensure that it supports the updated mandate. The pursuit of these two objectives is executed through a number of functions which include:

a) Formulation and implementation of monetary policy

b) Implementation of prudential and macro prudential policies

c) Issuing and redemption of notes and coins

d) Holding and managing the external reserves of the country

e) Fostering the development of money and capital markets in Jamaica

f) Acting as banker and financial agent of the Government and

g) Acting as banker to deposit taking institutions.

3. CUSTOMERS OF THE CENTRAL BANK

It is recognized that only a portion of the participants in the financial system are direct customers or counterparts with the Central Bank. These include:

a) Central Government;

b) Public Bodies;

c) Commercial banks (as participants of the payment and settlement systems);
d) Primary Dealers (as the inter-facers in the market between secondary participants in Government of Jamaica (GOJ) instruments and BOJ instruments)

e) Authorized dealers and cambios that engage in the trading of foreign currency with the Central Bank;

f) Other regulatory bodies and central banks;

g) Approved overseas correspondents (i.e. foreign banks and other financial institutions approved by the Management Committee /Board of Directors of BOJ) as institutions with which the Central Bank can conduct business.

h) High Commissions and Embassies;

i) Multilateral agencies (including Foreign Missions);

j) Employees of the Bank of Jamaica;

k) Members of the public (restricted to “walk-in customers/ persons conducting the following one-off transactions)

   i. Buying into or encashment of their holdings of GOJ instruments;

   ii. Changing out coins for notes or notes for coins;

   iii. Surrendering notes and coins that are no longer in circulation;

   iv. Surrendering torn or mutilated JMD notes for replacement with new JMD notes issued by the Central Bank;

   v. Selling foreign currencies1 to the Bank;

   vi. Purchasing souvenir notes and coins and other items, 

   vii. Encashment of cheques drawn on the BOJ.

1 Only the currencies reflected in counter rates on the BOJ’s website https://boj.org.jm/market/foreign-exchange/counter-rates/. Note that BOJ does not sell foreign exchange to the public.
The Bank does not conduct business with shell banks. Therefore, where transactions are being conducted with, by or through the Bank, such dealings must only proceed if the Bank is satisfied that the transaction(s) does not/ do not involve a shell bank or other entity that is established or operates like a shell bank.

4. LEGISLATIVE FRAMEWORK AND SYSTEMS

The Central Bank is cognizant that it is exposed to ML/TF risks, by way of persons wishing to use the services offered by the Bank to facilitate the commission of money laundering, terrorist financing or some other form of 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 be subject to the anti-money laundering frameworks and systems contained in local legislation and international standards.

4.1 This initially included:
   a) The Money Laundering Act 1998
   b) The Money Laundering Regulations, 1998
   d) The CFATF 19 Recommendations
   e) The FATF 40 + 9 Recommendations
   f) The Basel Best Practices on Customer Due Diligence (CDD)

4.2 The aforementioned initial listing was subsequently expanded to now include the updated applicable local legislation and international best
practices principles as indicated below:

a) The Proceeds of Crimes Act (POCA), 2007 (amended 2013) (This Act was repealed and replaced the Money Laundering Act, 1998 and the Regulations thereunder)


g) The United Nations Security Council Resolutions Implementation (Reporting Entities) Regulations, 2019

h) The Bank of Jamaica (AML/CFT/CFP) and Management of Risks Guidance Notes 2018 (formerly The Bank of Jamaica AML/CFT Guidance Notes, 2009\(^2\))

i) International Standards – The FATF 40 Recommendations, 2012\(^3\) and The Wolfsberg Principles on correspondent banking and on PEPs.

\(^2\) These Guidance Notes were first issued in 1995 and were updated and re-issued in 2004, and revised in 2007 and 2009. These Guidance Notes have since been updated in 2017 and will be re-issued when they have been published in the Gazette. These Guidance Notes can be accessed at the BOJ’s website https://boj.org.jm/wp-content/uploads/2020/02/Guidance_Notes_On_The_Prevention_Of_Money_Laundering_And_Countering_The_Financing_Of_Terrorism_Proliferation_And_Managing_Related_Risks.pdf

\(^3\) These Recommendations were formerly The FATF 40 +9 Recommendations that were re-issued in 2012 as The International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – The FATF Recommendations and continue to be periodically updated.
5. **RISK BASED FRAMEWORK**

5.1. As can be seen from Paragraph 3 above, the profile of 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. As such the AML/CFT/CFP 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 that are currently subject to local statutory and/or global standard AML/CFT/CFP obligations, and in the case of Central Government, additional obligations regarding anti-corruption laws, transparency and fiscal responsibility.

5.2. Under the revised FATF Forty (40) Recommendations, 2012 countries like Jamaica are required to identify, understand and assess, the money laundering and terrorist financing risks posed to the country. That assessment will therefore inform the overall national AML/CFT/CFP strategy and framework for a country to ensure that the measures applied to prevent or mitigate ML and FT are commensurate with the risks identified.

5.3. Jamaica conducted a national risk assessment in 2015 and the report was finalized in May 2016. A summary of that report was shared with Bank of Jamaica in August 2016. In relation to the financial sector, the key threats, risks and vulnerabilities identified to that sector and which are pertinent to the Central Bank were as follows:

   a) The existence of financial service providers who are unregulated for ML and TF purposes and whose services are used by unsophisticated customers who are less aware of AML/CFT/CFP risks;

---

4 The Integrity Commission Act, 2017 (which came into effect 22 February 2018) requires public servants earning above a certain income bracket to file annual asset declarations with the Office of the Integrity Commission. This Act repeals certain parts of the Corruption Prevention Act and accordingly replaces the previous obligation to make asset declarations under The Corruption Prevention Act, 2002.

5 FATF Recommendation 1 and Interpretive Note to Recommendation 1 (NB. This recommendation was revised in October 2020 to include a requirement for countries to identify and assess the risks of non-compliance with obligations related to Targeted Financial Sanctions to combat the Financing of the Proliferation of Weapons of Mass Destruction.)
b) Financial services that may be prime candidates for being abused for AML/CFT/CFP purposes but which are not compliant with their AML/CFT/CFP obligations;

c) Under-resourced regulators which can impact the effective oversight of FIs’ compliance with their respective AML/CFT/CFP obligations; and

d) Designated non-financial businesses recognized in the international standards as services, which should be regulated for ML and TF purposes, but which are not regulated in Jamaica for ML and TF purposes.

5.4. Risk Based Approach (RBA) for the Central Bank

In the context of the key threats, risks and vulnerabilities identified above, the assessment of risk should be:

a) informed by:

i. national risk assessment/(s) (if available) or other assessments available from the national authorities and agencies in relation to any sector; as well as peer review assessments (such as mutual evaluation reports) and financial sector assessments (FSAP reports); (Some financial institutions have accounts with the Central Bank while other financial institutions conduct other business with the Central Bank. A deficiency in their respective regulatory oversight or internal AML/CFT/CFP measures can increase the exposure of the Central Bank to ML and TF risks by virtue of its relationship with those institutions), and

ii. where applicable, assessment findings communicated by the Bank’s Corporate Risk Management Department in accordance with the Bank’s Policy document on Corporate Risk Management Framework\(^6\).

---
\(^6\) Corporate Risk Management Framework, November 2018
b) undertaken on an ongoing basis to take account of new risks and changing circumstances and must therefore be undertaken periodically with the frequency depending on the prevailing circumstances, and assessments must be documented (i.e. “be in writing”);

c) undertaken so that there is a clear identification, determination and understanding of the risks involved;

d) based on practical, comprehensive and up-to-date understanding of threats;

e) inclusive of commensurate measures that are clearly defined and applied;

f) approved by the respective authority/(ies) within the Central Bank for the governance and oversight of the relevant Divisions, documented and made available to officers and employees or staff where commensurate with respective functions, to allow for the identified measures to be applied and monitoring to be undertaken; and

g) readily available to the internal and external auditors of the Central Bank.

6. RISK ASSESSMENT GUIDE

In undertaking its assessment, where a higher risk scenario is identified by the Central Bank, enhanced measures should be applied to address such higher risks.

6.1. For the Central Bank, the main AML/CFT/CFP risks stem from the possibility of:

a) Corrupt officers and employees;

b) Undue influence from the private sector or politically exposed persons;

c) Use of the Central Bank’s services to commit or facilitate the commission of money laundering or terrorist financing.
6.2. However, for the Banking Department within the Central Bank, specific potential AML/CFT/CFP operating risks stem from:

a) Officers and staff not being aware of their respective AML/CFT/CFP related responsibilities;

b) Doing business with politically exposed persons (external to the BOJ) as well as with BOJ officers or members of staff (employees) without engaging the requisite safeguards and controls;

c) Absence of, or incomplete information provided by Government agencies or other customers seeking to transact business with or through the Central Bank, which can result in transactions involving listed entities or countries to which targeted financial sanctions or other countermeasures should be applied, being conducted or facilitated by the Central Bank;

d) Financial institutions not complying with their respective AML/CFT/CFP obligations thereby unwittingly exposing the Central Bank to AML/CFT/CFP related consequences such as de-risking by correspondent banks; or illicit proceeds being commingled with funds held by the Central Bank on behalf of these financial institutions;

e) Establishing or maintaining relationships with correspondent banks or with respondent banks that have weak AML/CFT/CFP controls; or which operate in jurisdictions that are subject to sanctions (e.g. UN list of jurisdictions which support terrorism; or proliferation of weapons of mass destruction); or which are subject to substantial AML/CFT/CFP related investigations or sanctions; or whose management or ultimate beneficial ownership raises AML/CFT/CFP concerns; or which is held in a group with an opaque holding structure;

f) Transactions attempted or conducted with counterfeit notes;

 g) Transactions attempted or conducted using forged signatures;
h) High cash value transactions;

i) Handling mutilated bank notes;

j) Transactions conducted with overseas counterparts that may have facilitated a financial crime or which are subject to AML/CFT/CFP investigations by the regulator or other authority in the overseas jurisdiction.

6.3. The Central Bank facilitates a high number of transactions involving changing out of local coins for Jamaican dollar notes. The Bank is not aware of any typology that has been identified to date which involves the use of coins. However, the requisite due diligence that applies to transactions undertaken with the Central Bank, will continue to be applied to these transactions as well, unless specifically indicated otherwise in this policy.

6.4. The requisite risk assessments must therefore be undertaken as indicated at paragraph 5.4 above. This means properly identifying the respective threats, risks and vulnerabilities of operating as a Central Bank and of operating as the Banking Department of the Central Bank, as well as the ability to respond effectively and in a timely manner to emerging issues (e.g. business transacted using electronic messaging and electronic transfers; the rise in cybercrime and the fast-changing typologies in relation to money laundering and the financing of terrorism.

6.5. Threats and Vulnerabilities

a) Threats
   i. ML and TF methods and trends;
   ii. Increase in cyber related crimes;
   iii. Economic, geographical or social environment factors;

---

7 The Central Bank is not a permitted person within the meaning of Section 101A of the POCA (a person shall not – “pay or receive cash in excess of the prescribed amount in a transaction for the purchase of any goods or services or for the payment or reduction of any indebtedness, accounts payable or other financial obligation”), and is therefore not authorized to conduct cash transactions in excess of the cash transaction limit of JMD 1 million.
b) Vulnerabilities i.e. variables relating to the regulatory, institutional and economic environment in the Central Bank or within which the Central Bank operates, in short, the overall Central Bank’s vulnerability versus:

   i. the Central Bank’s ability to prevent the use of its services to commit or facilitate ML and TF weaknesses or gaps in AML/CFT/CFP laws and regulations and in the national infrastructures (e.g. ID infrastructure, STR collection and analysis);

   ii. The weaknesses and gaps in existing in-house defense mechanisms (i.e. internal controls; adequacy and capacity of resources) to prevent ML and TF;

   iii. Lack of awareness, commitment, knowledge, resources in-house and in the wider national AML/CFT/CFP framework - particularly amongst clients of the Central Bank⁸;

   iv. Existence of causal relations amongst vulnerability factors (e.g. improper prioritization of issues; weak enforcement culture; high staff turnover and slow replacement of lost skills and trained persons ;)

   v. Substantial reliance on manual systems to support preventive measures.

The product of that exercise, which is the assessment, should achieve the objective of effectively identifying the Central Bank’s risks and give good guidance on where to focus the resources of the Central Bank to best address its AML/CFT/CFP risks.

7. **MAJOR AML/CFT/CFP POLICY ELEMENTS FOR THE CENTRAL BANK**

The following are the major AML/CFT/CFP related policy elements:

7.1. **Internal Controls Covering all Aspects of Operations**

⁸ See paragraph 3
a) Fit and proper requirements for staff and recruits
b) Anti-bribery and Corruption
c) Post-employment Conditions
d) Adherence to Policy and Procedures and ongoing review of these Policies and Procedures
e) Annual Training requirements for critical officers (including the Board and senior management) and for frontline staff in the Banking Department
f) Records Retention Policy
g) Cybersecurity
h) Relationship with audit, risk and compliance functions

i. Required disclosures\(^9\) (i.e. Suspicious transactions reporting and threshold transactions reporting\(^10\))

ii. Know Your Customer (KYC) and Customer Due Diligence (CDD)

7.1.1. Fit and Proper Checks\(^11\)

Checks for fitness and propriety entail more than a background check. It is a detailed review of the affairs and characteristics of the whole person to determine their fitness and propriety. Section 3 of the BOJ AML/CFT/CFP Operating Procedures\(^12\) provides details on "Internal Controls - Fit and Proper Checks".

It is important to note however, that the Bank of Jamaica Act does not expressly require that a fit and proper process be applied to prospective staff or prospective senior management appointments,

---

\(^9\) POCA section 94; TPA section 16
\(^10\) POC (MLP) Regulations, regulation 3
\(^11\) See for e.g. the BOJ’s Fit and Proper Guide for licensees under the BSA at www.boj.org.jm; See also the main assessment criteria in the FCA’s Handbook at www.handbook.fca.org.uk
but the recent amendments to the Act extend fit and proper requirements to Board members\textsuperscript{13}. However, all applicants eligible for employment with the Central Bank are subject to stringent due diligence background checks and would also be subject to police clearance checks. Thereafter, the Central Bank ensures on an ongoing basis, through various measures (compliance with policies, procedures; statutory obligations; general laws of Jamaica, disciplinary action track record; management of personal financial affairs, etc.) that staff and senior officers remain eligible for continued employment with the Central Bank. Employees therefore are required to abide by the Central 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 Central Bank commences.

\textbf{7.1.2. Anti-Bribery and Corruption Prevention}

The HR Policy Manual\textsuperscript{14}, 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

\textsuperscript{13} The BOJ Act was amended in December 2020 to, among other things strengthen governance arrangements to ensure these can support the Bank’s mandate. Among the amendments passed is a fit and proper requirement for members of BOJ’s Board and Statutory Committees.

\textsuperscript{14} See Appendix III for Applicable extracts from the Human Resource (HR) Policy Manual.
Central Bank, that employee is barred from, among other things, undertaking investments in the shares of deposit-taking licensees or its affiliates/subsidiaries.

7.1.3. Post-Employment Conditions
Currently, there is no restriction (in the governing statute or in the policies of the Central Bank) that expressly restrict employment of a departing officer or employee (regardless of rank) with a particular private or public sector employer. However, the Banking and Currency Operations Division (BCOD) and Market Operations Division (formerly one division known as the “Banking and Market Operations Division” (BMOD)), which are critical information sensitive areas, in practice employ certain precautions once notice of resignation is received from employees in those areas. The precautions include: –

a) Foregoing the typical notice requirements for resigning officers and employees and allowing the officer or employee to give immediate effect to the resignation;

b) Restriction of access to sensitive data or information (including being barred from attending meetings);

c) Restriction of access to the internal intranet service;

d) Removal from the list of employees and officers to whom general internal notices and advisories are issued;

e) Reduction of on-line access and internet privileges; and

f) Revision of work streams to focus on finalizing on-going matters and projects and identifying nominees to whom the matters and projects will be re-directed or re-assigned expeditiously.

The foregoing actions are dependent on a number of factors including - whether the departing officer or employee intends to remain in the public sector or to join the private sector, and the
circumstances of separation.

7.1.4. Adherence to Policies and Procedures

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

a) Contract Awards Procedures

In relation to contracts to be awarded in the course of the Central Bank’s maintenance, development and upgrading of its infrastructure – while external monitoring by the Public Procurement Commission, formerly the National Contracts Commission, is done in relation to contracts that reach or exceed JMD30 million, internal monitoring of all such matters is undertaken by a formally constituted Contracts Committee headed by the Deputy Governor, Finance, Technology and Administration.

The Bank is also subject to transparency requirements to disclose to the Contractor General all contracts valuing JMD500,000 and upwards. These disclosures must be made every quarter.

b) Financial Statement Standards and Publication Requirements

In relation to the Bank’s financial statements, the Bank is subject to statutory publication requirements. 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.

---

15 See [www.ppc.gov.jm/ppc](http://www.ppc.gov.jm/ppc)

16 Circular 27 Ministry of Finance and the Public Service (Public Expenditure Policy Co-ordination Division)

7.1.5. Annual Training Requirements for Critical Persons - AML/CFT/CFP Training

a) All employees are subject to this AML/CFT/CFP policy and should therefore familiarize themselves with the contents and with the requirements of this policy.

b) Employees should be aware of the serious nature of money laundering crimes and terrorist financing activities as well as proliferation financing, and should acquaint themselves with the provisions in the POCA on money laundering; the provisions in the TPA on terrorism financing as well as the preventive measures to which financial institutions and other regulated businesses are subject under the POC(MLP) Regulations, and under the TP (Reporting Entities) Regulations and the provisions of the UNSCRIA and the Reporting Entities Regulations thereunder. While the matter of taking the time to be aware of the subject of AML/CFT/CFP rests with employees, the Central Bank undertakes the responsibility of routinely sensitizing employees on matters which are pertinent to their employment through its Training and Learning & Development Programmes and Initiatives. Accordingly, all employees should be exposed to Anti-Money Laundering, Counter Terrorist Financing and Counter Proliferation Financing Programmes. Currently, the Central Bank specifically ensures that employees within the Banking Department (i.e. employees on the frontline who routinely interface with the members of the public conducting financial transactions with the Central Bank) are exposed to AML/CFT/CFP training at least once per year. Additionally, employees within the regulatory functions of the Central Bank are routinely exposed to AML/CFT/CFP training to ensure the awareness and experience of these employees remain relevant and appropriate to undertake the regulatory AML/CFT/CFP oversight of financial institutions which
are supervised or regulated by the Central Bank\textsuperscript{18}.

c) For financial institutions and other regulated businesses under the POCA, and reporting entities under the TPA, training is a statutory mandate\textsuperscript{19} and is critical for those entities to ensure that their employees remain knowledgeable on the statutory obligations of these entities; and that they employ the necessary measures effectively to prevent their respective services from being used to facilitate money laundering and terrorist financing.

d) Notwithstanding that the Central Bank is not a regulated business under the POCA, the Central Bank must still bear in mind the statutory defence that can be raised by an employee who has been charged with breaching certain provisions of the POCA. Under the POCA, a defence can be raised by an offending employee that the requisite training was not provided to him or her by the employer\textsuperscript{20} (See also the BOJ AML/CFT/CPF Guidance Notes\textsuperscript{21} – paragraphs 254 – 256).

e) In developing training programmes\textsuperscript{22}, particular emphasis should be placed on:

   i. **Employees on the front line** - The first point of contact of an institution with potential money launderers or persons attempting to finance terrorist activities is usually through employees who deal directly with the public. ‘Front-line’ employees (such as Tellers, Cashiers

\textsuperscript{18} 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. Training is also a requirement for staff of the Payment Systems Department who currently monitor Electronic Payment Systems Providers (i.e. non-bank service providers).  
\textsuperscript{19} POC (MLP) Regulations, regulation 5(1)(c); and TPA section 18(2)(c).  
\textsuperscript{20} See the POCA section 94(6)  
\textsuperscript{21} The AML/CFT/CPF Guidance Notes can be viewed at the BOJ’s web site https://boj.org.jm/wp-content/uploads/2020/02/Guidance_Notes_On_The_Prevention_Of_Money_Laundering_And_Countering_The_Financing_Of_Terrorism_Proliferation_And_Managing_Related_Risks.pdf  
\textsuperscript{22} See Paragraph 1(b) of Interpretive Note to FATF Recommendation 18. See also Paragraphs 246 and 255-259 of the BOJ AML/CFT/CPF Guidance Notes)
and Foreign Currency Staff, possibly also security personnel and receptionists for the banking area of the Central Bank or other members of staff who engage in negotiations of financial transactions nature with suppliers or third parties) 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 Appendix V of this policy. Frontline employees 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 Central Bank’s policy for dealing with occasional customers and ‘one off’ transactions, particularly where large cash transactions or unusual 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 frontline or other relevant staff. Such training must include familiarization with the offences and penalties arising under the POCA, the POC (MLP) Regulations, the TPA and the UNSCRRIA, typologies and management’s specific responsibility vis-à-vis dealings with ‘high risk’ transactions or business relationships.

iii. **New Employees** - should, as soon as possible, be exposed to basic AML/CFT/CFP sensitization, i.e., the
Central Bank’s AML/CFT/CFP policy- and overview of the laws, and made aware of the AML/CFT/CFP authorities, i.e., Competent Authorities for financial institutions and the Designated Authority under the AML/CFT/CFP laws.

f) **Training generally covers:**
   
i. The legislation and international standards discussed in paragraph 7.1e above.

   ii. The recognition or detection of unusual, irregular or suspicious information or matters as well as transactions that would meet the description of suspicious or which exceed the statutory threshold and which would normally be reported as STRs or TTR’s under Section 94 or 95\(^{23}\) of the POCA or Section 16 of the TPA.

   iii. Practical in-house scenarios and the appropriate reaction to such scenarios, real life examples of issues identified and reactions or responses applied.

   iv. The KYC requirements for customers, counterparties and other persons with whom or with which the Central Bank interfaces on a regular basis and which include:
      
      - Identification requirements
      - Agent authorization requirements
      - Verification of the customer’s/counterparty’s information
      - Verification of source of funds and source of

\(^{23}\) Refer to Threshold Transaction Report form under the POCA (MLP) Regulations. Hard copies available at the Government Printing Office of Jamaica. This can also be done electronically via [https://www.fid.gov.jm/](https://www.fid.gov.jm/).
wealth details

- Purpose of transaction requirements

v. Transactions that require senior management authorization;

vi. Procedures to make reports to the Nominated Officer and Senior Nominated Officer;

vii. The treatment of transactions deemed unusual, irregular or suspicious;

viii. Conduct that might constitute “tipping off”

Under the POCA a tipping off offence occurs where there is a disclosure in relation to a required disclosure that has been or is to be made; or where there is a disclosure in relation to a money laundering investigation that is being or is about to be conducted. (See Section 97) Under the TPA a terrorism offence (akin to “tipping off”) occurs where there is an unauthorized 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; or where there is an unauthorized disclosure of information or any other matter relating to an investigation.

Training is conducted on an on-going basis and is usually undertaken in a class room setting using in-house or external trainers or accredited AML/CFT/CFP on-line programmes. A certificate of satisfactory completion of the employee’s training in

---

24 Proceeds of Crime (Amendment) Act, 2019 Section 6 which amends section 97.
25 See Section 17 of the TPA
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 e.g.–

1. Employment;
2. Promotion/lateral movement to sensitive or frontline duties;
3. Expiration of minimum period since last training session which triggers refresher requirements.
4. Passage of new AML/CFT/CFP legislation or amendments to existing AML/CFT/CFP legislation;
5. Change in international best practice standards and requirements;
6. Revision to the BOJ AML/CFT/CFP Guidance Notes
7. Revision to the BOJ AML/CFT/CFP Policy

7.1.6. Training for the Executive Management and Board of the Central Bank

As a customer accessing financial services from overseas correspondent financial institutions, BOJ is required, based on Basel Committee on Sound Management of ML and TF Risks\textsuperscript{26}, to demonstrate that as a corporate customer it adheres to good governance practice which means having Board approved AML Policies and Board members who are aware of the international standards on ML/FT and PF, and the steps taken by BOJ to ensure its

\textsuperscript{26} See Basel Committee on Sound Management of ML and TF Risks, (2014) revised 2016 and published 2020 – Paragraph 17 Proper Governance Arrangements. (NB. For FIs and DNFBs the relevant standard is FATF R18)
services and facilities are not abused to commit, further or facilitate ML/FT/PF or any other financial crime.

In this regard, the Executive Management and Board of the Central Bank should also ensure they respectively receive adequate and appropriate exposure to the local AML/CFT/CFP laws and framework, as well as the international standards and best or sound practices, which impact AML/CFT/CFP obligations for financial institutions and designated non-financial institutions.

**7.1.7. Records Retention Policy**

Record keeping efforts for the purposes of this Policy should be guided by the requirements applicable to regulated businesses under the Proceeds of Crime Act, reporting entities under the Terrorism Prevention Act and the regulations under these statutes (see paragraphs 9.2b to 9.2d for details).

**7.1.8. Cybersecurity**

As indicated in paragraph 6.4 above, the requisite risk assessments must be undertaken to properly identify the respective threats, risks and vulnerabilities of operating as a Central Bank and of operating as the Banking Department of the Central Bank, as well as the ability to respond effectively and in a timely manner to emerging issues, such as business transacted using electronic messaging and electronic transfers; the rise in cybercrime and the fast-changing typologies in relation to money laundering and the financing of terrorism.

**7.1.9 Relationship with Audit, Risk and Compliance Functions**

a) Audit Review of AML/CFT/CFP Internal Controls

An assessment of the adequacy of the Central Bank’s AML/CFT/CFP
internal controls is to be undertaken by the internal audit function of the Central Bank. The Nominated Officer’s effectiveness in monitoring the Central Bank’s compliance with this AML/CFT/CFP policy and with the AML/CFT/CFP laws, regulations and industry best practices are therefore 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 actions where necessary, are taken in a timely manner. The Banking Department and all Departments within the Central Bank are subject to reviews by the internal audit function as well as external audit functions.

b) In addition, in keeping with FATF Recommendation 18\textsuperscript{27}, an independent assessment of the adequacy of the Central Bank’s AML/CFT/CFP internal controls is to be undertaken every two years by an external auditor.

c) The recommendations of the internal audit or the external audit (as the case may be) are to be implemented within the timelines specified in the respective recommendations.

7.1.10 The Senior Nominated Officer and the Nominated Officer

a) Best practice indicates that the compliance officer should function at a sufficiently senior level to effectively monitor the entity’s compliance with its AML/CFT/CFP functions; report to the Board of the entity and be sufficiently independent of the operations of the entity to maintain objectivity in undertaking the compliance oversight function.

b) In the Central Bank’s case, the compliance function is undertaken by a Senior Nominated Officer (SNO) and by the Nominated

\textsuperscript{27} FATF Recommendation 18 looks at internal controls and foreign branches and subsidiaries
Officer (NO). The function of the SNO\textsuperscript{28} is undertaken by the Senior Executive with responsibility for Banking and Currency Operations. The function of NO is undertaken by the Director of the Banking Department. Both officers occupy senior management positions in the Central Bank and both positions can also be viewed as integrally involved in the operations of the Central Bank.

The decision for the functions of the SNO\textsuperscript{29} and NO to be undertaken or to continue to be undertaken by the Senior Executive with responsibility for Banking and Currency Operations and by the Director of the Banking Department respectively, must each be ratified, by the Board of the BOJ.

c) It should however be noted that: -

i. The Central Bank is not a regulated business under the POCA or a reporting entity under the TPA which permits greater flexibility in establishing its nominated officer regime.

ii. The banking function within the Central Bank supports the main operations of the Central Bank – which are implementing monetary policy and overseeing financial stability (See paragraph 2i p.2)

iii. Neither the Senior Executive with responsibility for the Banking and Currency Operations nor the Director of the Banking Department is the sole decision-making body involved in the main operations of the Central Bank;

iv. The Central Bank is not a market participant in the offer of banking, financial or any other services to the public on a commercial basis. Its services to the public are confined to

\textsuperscript{28} This appointment of the current Senior Executive with responsibility for the Banking and Currency Operations Division was effective 1\textsuperscript{st} July, 2019. The appointment of the previous SNO was effective 11 October, 2006 and ended in 2019. The appointment of the current Director for the Banking Department was effective 9 September 2019.

\textsuperscript{29} Details of the functions of the SNO and the NO are outlined in Section 3.2 of the BOJ AML/CFT/CFP Procedures.
services in keeping with the BOJ’s statutory function as issuer of legal tender. In the Central Bank’s view, these factors differentiate the Central Bank from other financial institutions in Jamaica.

7.2. Required Disclosures

7.2.1. Reports to the Designated Authority

Notwithstanding that the Central Bank is not a regulated business under the POCA, the Bank subscribes to the requirement therein where an employee in the course of undertaking his or her functions (whether through the Banking Department or otherwise), becomes aware of information or a matter resulting in a knowledge, belief or suspicion that another person has engaged in money laundering or terrorist financing, there is an obligation for such information or matters relating to that knowledge, belief or suspicion that another person has engaged in money laundering or terrorist financing, to be reported. Additionally, as the Central Bank has committed to employing and applying policies in keeping with the national AML/CFT/CFP requirements and with applicable international standards, the Central Bank also subscribes to filing threshold transaction reports (within the meaning of the POCA) to the Designated Authority as follows:

7.2.1.1. Threshold Transactions

a) Under the POC (MLP) Regulations (r. 3(1)), Threshold Transaction Reports (TTRs\textsuperscript{30}) must be prepared for transactions in cash (i.e. currency) exceeding the stipulated threshold of USD15,000\textsuperscript{31} or

\textsuperscript{30} Refers to Threshold Transaction Report form under the POCA (MLP) Regulations, 2007 Hard copies available at the Government Printing Office of Jamaica. This can also be done electronically via https://www.fid.gov.jm/

\textsuperscript{31} Under the POCA (MLP) Regulations, 2007 (r. 3(8) the new limit for threshold reporting in the case of remittance companies is US$5,000.00. In the case of Cambios, reporting obligation in this regard remains at transactions
its equivalent in other currencies. However, given the types of transactions that are ordinarily undertaken by the Central Bank in relation to clearing banks or in the pursuance of its monetary policy mandate, it would not be reasonable for a TTR requirement to be applied by the Central Bank for transactions of that nature. It should further be noted that based on Jamaica’s exchange rate, a TTR transaction could also trigger the cash transaction limit under the POCA, which prohibits a person from undertaking transactions in excess of the statutory limit of JMD 1 million, in which case that transaction could not be facilitated by the Central Bank.

b) In relation to the Central Government, Statutory Bodies, Embassies and High Commission, it should be noted that transactions conducted by financial institutions with these authorities and bodies are statutorily exempt from the TTR requirement under the legislation. The Central Bank therefore takes a similar approach in relation to the treatment of transactions conducted with such authorities and bodies and a threshold transaction report will not be generated. However, if any transaction with such authority or body is one that ought to be flagged as suspicious, then a report should be made to the Designated Authority.

c) There are other transactions to which the TTR requirement could reasonably be applied (e.g. in relation to walk-in customers) and in this regard, the Central Bank does make TTRs to the Designated Authority. The reporting of threshold transactions to the Designated Authority should be made in writing and should amounting to and exceeding US$8,000.00. The revised reporting limits became effective on July 1, 2007.

32 Official transactions on behalf of the following institutions are exempt: Central Government, Statutory Bodies, Embassies and High Commissions.
contain all the information that is required on the statutory TTR form that is used by regulated businesses under the POCA\textsuperscript{33}.

The reporting regime for TTRs that apply for regulated businesses under the POCA are followed by the Central Bank. Accordingly, TTRs are to be submitted to the Designated Authority within five (5) business days after the end of each quarter.

The yearly reporting schedule for TTRs is as follows:

<table>
<thead>
<tr>
<th>Transactions for</th>
<th>Report within 5 Business Days after</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan – Mar</td>
<td>31 Mar</td>
</tr>
<tr>
<td>Apr – Jun</td>
<td>30 Jun</td>
</tr>
<tr>
<td>Jul – Sep</td>
<td>30 Sep</td>
</tr>
<tr>
<td>Oct – Dec</td>
<td>31 Dec</td>
</tr>
</tbody>
</table>

7.2.1.2. Suspicious Transactions

a) Matters of suspicion should be reported \textbf{promptly} to the Designated Authority to facilitate timely analysis and investigation or other action by that agency.

b) Employees must therefore always be alert to situations which may lead to money laundering and other illegal activities including the financing of terrorism. The types of transactions that may be used by a money launderer or by a person wishing to finance an act of terrorism or terrorist related activity group

\textsuperscript{33} Refer to Threshold Transaction Report form under the POCA (MLP) Regulations, 2007. Hard copies available at the Printers Office of Jamaica. This can also be done electronically via https://www.fid.gov.jm/

In keeping with the past practice of aligning the AML/CFT Policy with statutory requirements applicable to financial institutions BOJ will be issuing such reports in letter 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.
or person, are almost unlimited. However, in the case of money laundering, a suspicious transaction will often be one which is inconsistent with the customer’s known or legitimate business or source of funds or source of wealth (e.g. customer transacting business in amounts that exceed indicated salary or that exceed indicated means of earning an income). In the case of terrorist financing, such activities may occur with funds derived from legitimate sources, and as such the detection of such activities can be more difficult. Some indicators of terrorist financing include, transactions stemming from or involving jurisdictions that are flagged as high risk for terrorism; or transactions that are for the benefit of or undertaken by or with a person who is a listed entity (within the meaning of the TPA Section 14).

c) In relation to transactions conducted with the Banking Department, because the Central Bank is not a ‘deposit-taking institution’, its exposure to those money laundering or terrorist financing activities that could be perpetrated through accounts held with commercial financial institutions is therefore 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.

d) Employees within the Banking Department are therefore required to routinely enquire from transacting customers, information about the source of funds and source of wealth regardless of currency. The Banking Department personnel may be guided by Appendix V to this Policy which provides a list of activities that may be considered unusual or suspicious. In addition, Section 4 of the BOJ AML/CFT/CFP Operating
Procedures provides the list of “red flags” to which the Banking Department employees should, in particular, be alert.

e) It is important to 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. 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 enhanced due diligence and should in any event be advised to the Nominated Officer and still be reported to the Designated Authority.

7.2.2. The Required Disclosure Regime under POCA

The regime under POCA –

a) Reflects 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.

b) 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.

---

35. The FATF Recommendations reflect that FIs should be required to conduct enhanced customer due diligence measures, consistent with the risks identified. In particular, FIs should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious. Examples cited of EDD measures include obtaining additional information on the customer; intended nature of the business relationship, obtaining senior management approval to commence or continue the transaction; increasing the number and timing of controls applied to the account, selecting patterns of transactions that need further examination and requiring the first payment to be carried through an account with the customer’s name with a bank subject to similar CDD standards. – Paragraph 20 - Interpretation Note to R10.
36. See Section 94(1)(c), 94(4)(a) and 95(1)(c) of the POCA
37. See Section 94(2)(b) of the POCA
c) 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\(^{38}\);

d) Includes a statutory reporting form under the POC (MLP) Regulations, to facilitate the required disclosures filing – (See Form 1 of the Schedule to these Regulations\(^ {39}\)).

In keeping with the practice of aligning the AML/CFT/CFP Policy with statutory AML/CFT/CFP requirements applicable to regulated businesses under the POCA, the Central Bank adheres to the statutory reporting timeframes\(^ {40}\).

### 7.2.3. The Reporting Regimes under the TPA

The TPA requires that financial institutions:

a) determine on a continuing basis whether they are in possession or control of property owned or controlled by or on behalf of a listed entity. A listed entity is one which is either designated as a terrorist entity by the United Nations Security Council, or is an entity which the DPP has requested the court to designate as a listed entity on the basis of there being reasonable grounds to believe the entity has knowingly committed or participated in the commission of a terrorism offence; or is knowingly acting on behalf of, at the direction of or in association with such an entity\(^ {41}\);

b) report all suspicious transactions to the Designated Authority, which under the TPA is, the CTD of FID or such other person as the

---

\(^{38}\) See Section 94(2) of the POCA

\(^{39}\) See Appendix IV for Form 1 of the Schedule of the POC (MLP) Regulations

\(^{40}\) 1. See Appendix V for List of Examples of Unusual/Suspicious Activities

2. See Appendix II of the BOJ AML/CFT/CFP Operating Procedures for Sample Letter re: Section 100 Reports (Authorized Disclosures of suspicious activities (including suspicious transactions)

3. See Appendix VI for Some of the Offences under the required disclosure regime under the POCA

\(^{41}\) See Section 14 of the Terrorism Prevention (Amendment) Act
Minister may substitute by order, subject to Affirmative Resolution and published in the Gazette:\textsuperscript{42}:

c) ensure that high standards of employee integrity are maintained, and that employees are trained on an ongoing basis regarding their responsibilities under the Act:\textsuperscript{43};

d) establish and implement programmes, policies, procedures and controls for enabling them to fulfil their duties under the TPA:\textsuperscript{44}.

\textbf{Note: Under the TPA there is no TTR obligation.}


a) The Central Bank is not included in the definition of a financial institution under this Act and therefore is not subject to the express obligations placed on such persons under the Act. The UNSCRIA was passed in November 2013 and is designed to address compliance with Recommendation 7 (on Targeted Financial Sanctions related to combatting the financing of the proliferation of weapons of mass destruction) of the FATF Recommendations issued in 2012. The UNSCRIA forms the basis for Jamaica to respond to resolutions of the UNSEC by promulgation of the requisite Regulations under the Act. Currently Jamaica has promulgated the UNSEC Resolutions Implementation (Asset Freeze – Democratic People’s Republic of Korea) Regulations, 2013.

b) The Act imposes a duty on financial institutions and designated non-financial institutions to determine whether or not they are in possession of property for a person proscribed by regulations made

\textsuperscript{42} The Terrorism Prevention (Amendment) Act, 2013, new section 15(1) and new subsection (9).
\textsuperscript{43} Section 18 of the Terrorism Prevention (Amendment) Act.
\textsuperscript{44} Section 18 of the Terrorism Prevention (Amendment) Act.
under Regulation 3 and to report whether they are, or are not, in possession of property for a person who is so proscribed\textsuperscript{45}. These reports are to be made to the Designated Authority, which is defined in the Act, to be the CTD of the FID\textsuperscript{46}. Reporting in this regard must be done in compliance with any directions that may be given by the Designated Authority\textsuperscript{47}; and the fact that a report has been made must not be disclosed to any other person\textsuperscript{48}. These reports are due once every four calendar months. Reports are also due upon request of the Designated Authority\textsuperscript{49}.

c) It is important to note that the UN related requirements for countries are currently not risk based\textsuperscript{50} and do not require the full extension of the CDD/KYC obligations from the AML/CFT/CFP framework to combatting PF related obligations. (See also – Special Guidance Regarding UNSEC Resolutions on the Proliferation of Weapons of Mass Destruction – set out at Section V(B) of the BOJ’s AML/CFT/CFP Guidance Notes)\textsuperscript{51}

7.3. KYC and CDD

This refers to:

a) Proper customer identification elements

b) Source of funds for transactions exceeding USD 1,000 or the equivalent in any other currency.

c) Graduated Customer identification and KYC requirements

\textsuperscript{45} See Section 5 of UNSCRIA
\textsuperscript{46} See Section 5 (1) of UNSCRIA
\textsuperscript{47} See Section 5 (4) of UNSCRIA
\textsuperscript{48} See Section 5 (6) of UNSCRIA
\textsuperscript{49} See Section 5 (3) of UNSCRIA

\textsuperscript{50} This position has since changed with the revision of the FATF recommendation in October 2020 to include a requirement for countries to identify and assess the risks of non-compliance with obligations related to Targeted Financial Sanctions to combat the Financing of the Proliferation of Weapons of Mass Destruction.)

\textsuperscript{51} (See BOJ’s website https://boj.org.jm/wpcontent/uploads/2020/02/Guidance_Notes_On_The_Prevention_Of_Money_Laundering_And_Countering_The_Financing_Of_Terrorism_Proliferation_And_Managing_Related_Risks.pdf)
8. HANDLING SUSPICIOUS SITUATIONS

a) In terms of the handling of suspicious transactions, the measures outlined in paragraphs 268 and 271 of the BOJ AML/CFT/CFP Guidance Notes\textsuperscript{52} may be applied by the Central Bank (as far as possible) to the services offered through the Banking Department\textsuperscript{53}.

b) Although the Central Bank is not a financial institution listed in the TPA and has no express reporting obligations under the TPA, facilitating dealings of any kind with any property that is owned or controlled by a terrorist group or providing property of financial or other services knowing or intending that they be used for a terrorist purpose, is an offence under the TPA\textsuperscript{54}. Accordingly, where there is a suspicion that a matter is facilitating or amounts to terrorist financing, the Central Bank should not accommodate, conduct or complete the transaction and the matter should be reported to the Designated Authority\textsuperscript{55}.

c) The reporting of suspicious activities, which includes transactions considered suspicious to the Designated Authority, should be made in writing to the Designated Authority pursuant to Section 100 of the POCA\textsuperscript{56}. These reports should contain all the information that is required on the statutory STR form that is used by regulated businesses under the POCA, and by reporting entities under the TPA and such reports should be accompanied by any supporting documentation pertinent to the report.

---


\textsuperscript{53} See Section 5 of the BOJ AML/CFT/CFP Operating Procedures for further details on the handling of suspicious situations.

\textsuperscript{54} See Sections 4 and 6 of the TPA

\textsuperscript{55} See also – Special Guidance Regarding treatment of Listed Entities – set out at Section V(A) of the BOJ’s AML/CFT/CFP Guidance Notes) at: https://boj.org.jm/wpcontent/uploads/2020/02/Guidance_Notes_On_The_Prevention_Of_Money_Laundering_And_Countering_The_Financing_Of_Terrorism_Proliferation_And_Managing_Related_Risks.pdf

\textsuperscript{56} See Sample Letter (SAR) in Appendix II of the BOJ AML/CFT/CFP Operating Procedures.
9. COMPLIANCE AND CUSTOMER DUE DILIGENCE

9.1. Banking Services Offered Through the Banking Department of the Central Bank

9.1.1. Maintenance of Customer Service
It is important that in complying with the requirements of this policy, that employees at all times operate in a professional manner. In this regard, the consistent application of requirements is critical at all times regardless of the person involved in the transactions. Section 6 of the BOJ AML/CFT/CFP Operating Procedures provides further details on the maintenance of customer service.

Threats of any kind to the personal safety of the Central Bank’s staff should be immediately reported to the senior floor manager and the Nominated and Senior Nominated Officers 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/deviations in this regard take place, the process of addressing such departures/deviations will be informed by the applicable processes outlined in the HR Manual and with any other determinations made by the Central Bank.

9.1.3. Practical Operational Enforcement
There are certain steps (See details in Section 7 of BOJ AML/CFT/CFP Operating Procedures) that should be taken by employees when confronted with unusual or suspicious activities before proceeding to conduct the transaction. These include evaluating transactions, applying enhanced

measures where transactions appear to be unusual and taking into consideration the situation or the individual causing suspicion.

9.1.4. Cash Transaction Limits

9.1.4.1. Cash Transactions

By virtue of Section 101A (1) of the POCA, it is illegal for a person to pay or receive cash in excess of $1,000,000 in a transaction OR for a person to artificially separate a single activity or course of activities into a set of transactions so that each transaction involves a payment and receipt of cash that is less than $1,000,000, but which activity or course of activities in the aggregate involves payment and receipt of cash that exceeds the $1,000,000 limit.

The Central Bank is not a permitted person under the POCA and therefore cannot conduct or facilitate cash transactions that exceed the statutory JMD $1 million threshold.

For the avoidance of any doubt, the Central Bank does not consider the delivery of currency to and from the Bank or the bulk transportation of currency between the Bank and third parties, to constitute ‘payments for the purchase of any goods or services or for the reduction of any indebtedness, accounts payable or other financial obligations’.

9.1.4.2. Cross Border Transportation of Cash

When undertaking cross border bulk transportation of currency, the Central Bank’s arrangements and reports on these activities must

58 A permitted person is defined as a bank licensed under the Banking Services Act; a licensed deposit-taking institution that is regulated by BOJ; a person licensed under the BOJ Act to operate an exchange bureau; any other person that the Minister may, by order subject to affirmative resolution (see Proceeds of Crime Act Section 101A (6))

comply with the POCA and with any relevant reporting and other arrangements established by the Designated Authority under POCA.\textsuperscript{60}

9.1.5. Source of Funds and Source of Wealth Requirements

a) For the purposes of this policy, the requirement for a customer or counterparty to declare the source of funds prior to a transaction being conducted with the Central Bank is mandatory for all transactions. Accordingly, this policy requires that 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) that are being conducted with the Bank. However, based on the customer base and profile and type of counterparts with which business is routinely transacted by the Central Bank, the Bank may exercise its discretion in applying the requirement for e.g. using a threshold below which the requirement may not be applied or noting the circumstances in which the application of requirement is not or would not be practical. So for example, 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):

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

The Bank’s discretion will not be exercised for transactions that appear suspicious.

b) The source of wealth for a customer or counterparty must also be

\textsuperscript{60} Proceeds of Crime Act Section 101; The Proceeds of Crime (Report Under Section 101 As to Transportation of Cash) Order, 2010
declared prior to an account being established with the Central Bank.

i. Source of wealth refers to the origin of the assets the customer has and which may be the source of the funds used for a particular transaction.

ii. Source of funds refers to the origin of the particular funds or instrument that is relied on or used for a particular transaction and is therefore a subset of a customer’s wealth.

iii. The following examples of sources of wealth allow for a determination of net worth:

- Self-employment; employment with the public or private sector;
- Inheritance;
- Royalties;
- Investment portfolio;
- Winnings from games of chance;
- Successful payout from a lawsuit;
- Gifts

Examples of source of funds:

- Bank account
- Encashment of investment portion of insurance policies
- Sale of asset

c) Unless discretion is exercised, Senior Management with ultimate responsibility for banking operations within the Bank must ensure that the personal circumstances and the income sources for persons conducting transactions with the Central Bank are declared and the information is verified as far as possible.

d) In the case of customers who are also employees with the Bank, salary is the standard declaration of source of wealth and the source from which funds are used to transact business through accounts held with
the Bank. However, if funds from sources other than the salary of the employee will be flowing through the account, then the Bank should ensure that the non-salary-based source of wealth is obtained.

9.1.6. Customer Information\textsuperscript{61}

a) The identity of each person transacting business with the Central Bank must be established prior to the Central Bank proceeding to conduct or facilitate a transaction with that person. Procedures must therefore be in place for the recording and regular review of customer identification and transaction information/records to ensure that the information is current, valid and comprehensive, as well as the retention of such information for a minimum of seven years after the transaction was initiated/attempted or had actually taken place, or the business relationship has been terminated. In the case of customers who are already established or confirmed as employees of the Central Bank, reliance will be placed on the identification and verification due diligence procedures that have been done by the Central Bank’s Human Resources Department and, unless the circumstances warrant otherwise, the standard Central Bank Employee’s Identification card will be relied on as satisfactory evidence that the individual is who he or she claims to be.

b) Measures that will allow the Central Bank to understand the nature and purpose of a customer’s business\textsuperscript{62} or how the public body or entity with whom the Central Bank is, or will be conducting business, functions or operates, must be implemented. The measures should allow the Central Bank to establish a basis for determining whether a transaction is unusual or suspicious, or is consistent with the expected funds flowing through the account or the expected types of transactions, or is consistent with the

\textsuperscript{61}See POC (MLP) Regulations, Regulation 7(5); 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.

\textsuperscript{62}See POC(MLP) Regulations, 2007 Regulation 7(2)(a)
activity that would typically arise in the course of such a business, function or operation.

c) Measures should be implemented that allow the Central Bank to deal with special areas of operations such as high-risk counterparties (e.g. 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).

### 9.1.7. Identification of Natural Persons

a) 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:

   i. true name and names used;
   ii. correct permanent address, including postal address;
   iii. date of birth;
   iv. nationality;
   v. source of funds, and source of wealth;
   vi. contact numbers (work; home; cellular);
   vii. Taxpayer Registration Number (TRN)\(^3\)

b) The matters at (i) to (vii) above also apply to the individuals conducting business in the name of or on behalf of, or as an agent of

---

\(^3\) The Bank has advised the financial sector that under the POC (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. Additionally, note that transactions with the Government require presentation of a TRN.
the central government, a primary dealer, a commercial bank, cambio or an approved overseas correspondent bank. Employees doing business on behalf of another employee will be required to demonstrate to the satisfaction of the Banking operations that the transacting employee has the appropriate authority and the requisite authorization to act on behalf of another employee.

c) As regards the inclusion of the TRN requirement in the KYC details, the following should be noted:

i. Under the POC(MLP) Regulations (amended 2019) “customer information” is 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 and mother’s maiden name (in the case of a natural person) and, where applicable, the information referred to, at Regulation 13(c) (i.e. identity of beneficial owner), as well as information that will verify the nature of the customer’s business, trade or source of funds.

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 or produce in compliance with a customer information order. For more on the customer information order, see paragraphs 127 and 128 F of the BOJ AML/CFT/CFP Guidance Notes. The following are examples of acceptable forms of identification for individuals (other than employees) transacting business with the Central Bank:

i. Valid Driver’s Licence (bearing a photograph of the individual), issued by the authority in the country in which the person is resident;

ii. Valid Passport;

iii. Valid Voter’s Identification Card or

iv. Any other valid National Identification Card (bearing a photograph)

9.1.8. Identification of Corporate Bodies

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;

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

---

65 See also the BOJ AML/CFT/CFP Guidance Notes, 2018 which can be viewed at the BOJ’s web site https://boj.org.jm/wpcontent/uploads/2020/02/Guidance_Notes_On_The_Prevention_Of_Money_Laundering_And_Countering_The_Financing_Of_Terrorism_Proliferation_And_Managing_Related_Risks.pdf
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 and

j) TRN and Tax Compliance information

9.1.8.1. Government Companies

a) Items (f), (g) and (i) in paragraph 9.1.8 above would not be applicable in the case of a government company. However, all other information requirements applicable to a body corporate, apply to a government company.

b) Adequate information (including the requisite authorization to act for or in the name or on behalf of the Government company) 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.

c) Customer due diligence for corporate customers may be satisfied if the corporate customer has established to the Central Bank’s satisfaction that it is a company listed on the Jamaica Stock Exchange’s (“JSE’s”) public listing of companies and is in good standing with that body.

i. Good standing confirmations include ensuring the JSE or other stock exchange explicitly confirms:

---

66 Since December 2017, the Companies Act requires all companies to file ultimate beneficial ownership information with the Companies Office of Jamaica (See section 109(a), (aa) and (ab) of the Companies (Amendment) Act, 2017).
• That the filing of audited financial statements is prompt and up to date, the filing of audited financial statements does not apply to branches of financial institutions;

• That there are no pending disciplinary actions against the company;

• That no disciplinary action has been taken by the JSE or other stock exchange against the company within the last seven years; (disciplinary actions may include administrative fines; de-listing; mandatory suspension of trading in the shares of the company).

ii. Companies listed on more than one exchange must be in a position to provide the above confirmations from the respective exchanges on which the company is listed.

iii. This method of conducting customer due diligence on corporate customers is applicable only in respect of the company that is itself listed on the stock exchange and not in relation to its subsidiaries; holding company/ies/parent/s; or any other affiliates of the listed company.

iv. Where the corporate customer is a part of a group of companies, the Central Bank must ensure that it is aware of, and understands any group structures in which the corporate customer resides, and has undertaken the requisite due diligence to apprise itself of any relationships or activities (commercial and otherwise) within the group that could present a reputational risk to the Central Bank. When there is doubt concerning the identity of a company, its controllers, directors, shareholders or ultimate beneficial owners/shareholders, a search must be conducted at the Registrar of Companies or equivalent authority for
registration, the requisite trade or professional regulatory body or other appropriate source.

9.1.9. Central Government

Items (a) - (i) in paragraph 9.1.8 above would not be applicable in the case of Central Government, which term for the purposes of this policy means Ministries and Departments of Government. In the case of Central Government, reliance will be placed on the identification and verification due diligence procedures that have been done by the Central Government’s processes in relation to its authorized officers and agents unless the circumstances warrant otherwise and 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.

9.1.10. Statutory Bodies

Items (a), (b) (f), (g), (h) and (i) in paragraph 9.1.8 above would not be applicable in the case of a statutory body. However, information requirements at items (c) and (d) apply to a statutory body. Reliance will be placed on the identification and verification due diligence procedures that have been done by the statutory body’s processes in relation to its authorized officers and agents unless the circumstances warrant otherwise save and except that, adequate information (including the requisite authorization to act for or in the name or on behalf of the 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.
9.1.11. Deposit Taking Institutions

Deposit Taking Institutions are licensed under the Banking Services Act; regulated by the Central Bank; and subject to the POCA, the TPA, the UNSCRIA and regulations, statutory AML/CFT/CFP requirements under these statutes, as well as the BOJ’s AML/CFT/CFP Guidance Notes. Additionally, most of the DTI’s are wholly held by a parent company that is listed on the Jamaica Stock Exchange and each DTI is a person to whom Regulation 10 of the POC (MLP Regulations and of the TP (Reporting Entities) Regulations apply. Reliance may therefore be placed on the identification and verification due diligence procedures that have been done by the DTI’s processes in relation to its authorized officers and agents, unless the circumstances warrant otherwise and save and except that, adequate information (including the requisite authorization to act for or in the name or on behalf of the financial institution) 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. Complete and up-to-date notices of changes in officers acting on behalf of the commercial bank should therefore be provided to the Central Bank.

9.1.12. Authorized Dealers (“ADs”)

ADs are persons to whom the widest authorization under the Bank of Jamaica Act to conduct dealings (i.e. buying, selling, borrowing or lending) in relation to foreign currency or foreign currency instruments have been granted. The designation as “Authorized Dealer” is conferred by an order.

---

67 Bank of Nova Scotia Jamaica Ltd.; National Commercial Bank Ja. Ltd.; Sagicor Bank (Ja) Ltd.; First Caribbean Bank (Ja) Ltd.; JMMB Bank Ltd.; First Global Bank Ltd. NB. (Re: the other commercial banks - Citibank N.A. [Ja] is the local branch operation of Citibank NA New York, and JN Bank is the wholly held subsidiary of JN Group a company whose shares are mutually held by the members of the JN Group.)

68 Regulation 10 stipulates that where a payment is to be made by an applicant for business and it involves debiting an account held with a bank, the fact that that payment is debited from an account held with the bank constitutes the required evidence of that applicant for business’ identity for the purposes of the Regulations.

issued by the Minister of Finance and the Public Service pursuant to Section 2 of the Bank of Jamaica Act. Currently the designation of Authorized Dealer has only been conferred on deposit taking institutions within the meaning of the Banking Services Act. Accordingly, all commercial banks, merchant banks and building societies are authorized dealers. With the exception of being wholly held by a parent company that is listed on the Jamaica Stock Exchange, ADs bear all other characteristics described above for DTIs. Reliance may therefore be placed on the identification and verification due diligence procedures that have been done by the AD’s processes in relation to its authorized officers and agents, unless the circumstances warrant otherwise and save and except that, adequate information (including the requisite authorization to act for or in the name or on behalf of the financial institution) 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. Complete and up-to-date notices of changes in officers acting on behalf of the AD should therefore be provided to the Central Bank.

9.1.13. 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/CFP requirements under the POCA, the TPA, the UNSCRIA and regulations under these statutes as well as the FSC AML/CFT Guidelines. The designation as “Primary Dealer” is conferred by a certificate of designation issued by the Government of Jamaica and the Central Bank to securities dealers who meet the Central Bank’s fit and proper criteria. Reliance may therefore be placed on the identification and verification due diligence procedures that have been

---

70 The BOJ’s fit and proper criteria are based on the F&P Criteria which applies to licensees under the BOJ Act (section 22B (exchange bureau) and section 22G (money transfer and remittance agents and agencies). These criteria are informed by the criteria outlined in section 3 of the BSA and the assessment process involves checking with the banking sector regulatory arm of the BOJ known as “the Supervisory Department”.

46
done by the Primary Dealer’s processes in relation to its authorized officers
and agents, unless the circumstances warrant otherwise and save and
except that, adequate information (including the requisite authorization to
act for or in the name or on behalf of the Primary Dealer) 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. Complete and up-to-date notices
of changes in officers acting on behalf of the Primary Dealer should
therefore be provided to the Central Bank. The list of Primary Dealers can
be found at the Central Bank’s website at https://boj.org.jm/.

9.2. General Customer Due Diligence

a) In addition to the foregoing, there should also be periodic updates of
customer information at least once every seven years. The procedures
for the establishment and implementation of transaction verification are
outlined in Section 8 of the BOJ AML/CFT/CFP Operating Procedures.

b) Record keeping efforts for the purposes of this Policy should be guided by
the requirements applicable to regulated businesses under the Proceeds of
Crime Act, reporting entities under the Terrorism Prevention Act and the
regulations under these statutes.

c) At a minimum, a record must be kept of the following: -

i Identification information and related verification efforts;

ii The identities of principals and agents must be obtained in the
case of transactions being conducted by a person on behalf of
another;

iii Customers who are PEPs and related verification efforts;

iv Information on wire transfers and other electronic funds transfers

---

71 POC(MLP) Regulations (R. 7(1)[c] & [d].)
73 See also POC(MLP) Regulations, (Regulation 11, 12 and 13)
conducted with or by the Central Bank as outlined in Regulation 9;

v Transaction records, and related verification efforts (where applicable);

vi Business correspondence,

vii Reviews and due diligence undertaken where there is a suspicion of ML or FT (the methodology used; details of efforts made, persons spoken with and documents and information accessed and findings and conclusions must also be documented and made available for investigations of ML/FT or other financial crimes; and to facilitate audits of the Bank’s AML/CFT mechanisms).

d) Anonymous, fictitious accounts or numbered accounts must not be maintained by the Central Bank.\textsuperscript{74}

9.3. High Risk Transactions/Business Relationships

9.3.1. Politically Exposed Persons (PEPs)\textsuperscript{75}

PEPs are individuals who are or have been entrusted with prominent public functions.

a) This category of persons includes the following persons and their immediate family and close associates\textsuperscript{76}:

i. Heads of State or of Government,

ii. senior politicians,

\textsuperscript{74} See also regulation 16 of the POC (MLP) Regulation; and regulation 16 of the Terrorism Prevention (Reporting Entities) Regulations.

\textsuperscript{75} See FATF Recommendation 12

\textsuperscript{76} (See also Regulation 7A (6) of the POC (Money Laundering Prevention) Regulations; and regulation 6(A) (6) of the Terrorism Prevention (Reporting Entities) Regulations. Close associate means parent, siblings, spouse, children and in-laws as well as close associates i.e. persons known to maintain unusually close relationship with PEPS also included in requirement for enhanced scrutiny
iii. senior government officials,

iv. senior executives of state-owned corporations;

v. important political party officials; judicial or security force and/or military officials (whether elected or not);

vi. persons entrusted with a prominent function by an international organization (i.e. senior management – directors, deputy directors, and members of the board or equivalent functions)

b) Middle ranking or more junior individuals in the foregoing categories are not intended to be included in the designation or classification as PEP.

c) The POC(MLP) Regulations and TP (Reporting Entities) Regulations refer to the category of persons who in relation to any State, carries out functions analogous to any of the following:

i. a Head of State;

ii. a Head of Government;

iii. a member of any House of Parliament;

iv. a Minister of Government;

v. a member of the judiciary;

vi. a military official above the rank of Captain;

vii. a member of the police of, or above the rank of Assistant Commissioner;

viii. a Permanent Secretary, Chief Technical Director or Chief Officer in charge of the operations of a Ministry, Department of Government, Executive Agency or Statutory Body, (as the case may be)\(^7\)

ix. a Director or Chief Executive of any company in which the Government owns a controlling interest;

\(^7\) This category is interpreted as capturing local government officials from at least the rank of Mayor.
x. an official of any political party\textsuperscript{78};

xi. an individual who holds or has held a senior management position in an international organization, and

xii. an individual who is a relative or is known to be a close associate of a person described in sub-paragraph (a) or (b) above.

d) Based on the above criteria the individual who currently meets the description of a domestic politically exposed person (PEP)) is the Governor of the Central Bank\textsuperscript{79} i.e. chief officer in charge of the operations of a statutory body.

The BOJ’s Banking Department processes have been updated to formally incorporate PEP identification measures.

9.4. Additional Considerations\textsuperscript{80}

Given the risk assessment profile requirements under the AML/CFT/CFP regulations as well as the risk-based approach contemplated by the revised FATF Recommendations, extending the enhanced or heightened measures to persons who are not expressly reflected in the list at Regulation 7A(6)(a) of the POC (MLP) Regulations and at Regulation 6A (6) of the TP (Reporting Entities) Regulations, could be done. Persons who fall in this category could include former PEPs or middle ranking or junior officials acting in the name of, or on behalf of or for a PEP, if from the Central Bank’s own risk assessment, the profile of the person warrants such an approach to be taken. It is expected that in such cases, such a profile would be reflective of, any one

\textsuperscript{78} Any member of the Executive of a Political Party.

\textsuperscript{79} Regulation 7A(6)(a)(viii) of the POC (MLP) Regulations; and Regulation 6A(6)(a)(viii) of the Terrorism Prevention (Reporting Entities) Regulations.

\textsuperscript{80} See also the Wolfsberg Principles for additional reading on the topic of ‘PEPs’. For eg. PEP FAQ states viz. “that, the following may also be considered to fall within the definition (of PEPs) but may be excluded in areas where the risk of corruption or abuse is considered to be relatively low as they do not have the ability to control or divert funds. Heads of Supranational Bodies (eg. UN, IMF, WB) Members of Parliament, or National Legislatures, senior members of the Diplomatic Corps. Eg. (Ambassadors, Charges D’Affaires, Members of the Boards of Central banks)”
or more of the following -

a) whether the individual is an elected representative\(^81\) or not -

i. the individual carries out functions of a public nature, which permit access (directly or indirectly) to public property (including funds or benefits – whether in cash or kind) and which give the individual the authority to make decisions or issue directives regarding the use of public property; and

ii. the function undertaken by the individual exists in relation to an environment in which the risk of corruption or abuse is considered to be very high (e.g. little or no established procedures or protocols that are designed to implement stringent internal controls and accountability measures; absence of effective disciplinary sanctions or a framework which does not include penalties that are effective proportionate and dissuasive);

iii. the individual’s prominence or position (as a public figure) –

1) facilitates the ability to influence or control (directly or indirectly) the access to and/or use of public property (including funds or benefits – whether in cash or kind); an

2) the individual is either known to be corrupt or is suspected of being corrupt, or the individual’s name is associated with incidences of corruption or abuse; or

iv. the individual meets the criteria of a close associate of a person at 1, or 2, above.

b) It should be noted that a person who qualifies for classification as a

---

\(^{81}\) This category is interpreted as capturing local government officials from at least the rank of Mayor.
PEP can remain subject to an assessment of ‘high risk’ even after his/her appointment ends or is terminated as the basis for such treatment should be on assessed risk and not on prescribed time limits\textsuperscript{82}.

c) Using a risk-based approach presumes that based on the risk assessments conducted, providing relaxed measures (for persons meeting the category of a PEP) if the risk assessment confirms that the profile of the person warrants such an approach to be taken, would not be precluded. However, the AML/CFT/CFP regulations already specify the category of persons, who, from a national perspective, are deemed to be high risk\textsuperscript{83}. In relation therefore to those specified categories of persons, applying reduced or lenient measures should not occur unless that approach is specifically permitted in the AML/CFT/CFP laws.

d) A business relationship with a PEP should not be established if the Central Bank knows or has reason to suspect that the source of wealth disclosed or source of funds provided, derive from corruption or misuse of public assets. Senior management approval must also be obtained to continue an existing relationship with a person who becomes a PEP after the establishment of the relationship or whose status as a PEP is confirmed, realized or discovered subsequent to the establishment of the relationship. Senior management with ultimate responsibility for banking operations should ensure that information on the personal circumstances, income sources and sources of wealth of the PEP are

\textsuperscript{82} FATF Guidance on Politically Exposed Persons (R12 and 22) June 2013, “B” Time Limits of PEPs Status, paragraph 44, page 12.

\textsuperscript{83} Informed by factors such as – the 3rd round recognition of these persons as ‘high risk & possibly also by Jamaica’s performance on the corruption perception index published periodically by Transparency International. The corruption perceptions index measures the perceived levels of public sector corruption in 180 countries and territories. In 2018 Jamaica received a ranking of 70 out of 180 or was ranked in the 44th percentile. In 2020 Jamaica received a ranking of 69 out of 180 countries or was ranked in the 44th percentile.
obtained and verified as far as possible, and should also be alert to sources of legitimate third-party information. Whilst it is appreciated that efforts must be made to protect the confidentiality of PEPs and their businesses, these accounts must be available for review by the Central Bank’s Senior Nominated Officer and Nominated Officer and by the internal auditors. The approval of business relationships involving PEPs must be obtained from at least one member of the Central Bank’s Management Committee, in addition to the Director, Banking Department and the Division Chief, Banking and Currency Operations Division.

e) To mitigate the significant legal and reputational risk exposures that the Central Bank may face from establishing and maintaining business relationships with PEPS, or continuing existing business relationships with PEPs, appropriate procedures should be implemented and should be applied prior to the commencement or continuation of such relationships (See Section 9 of the BOJ_AML/CFT/CFP_Operating Procedures for further details).

f) Following the commencement of banking relationships, there should be:

i. Regular reviews of customer identification records to ensure they are kept current; and

ii. Ongoing monitoring of PEP accounts.

g) The procedures outlined in Section 9 of the BOJ_AML/CFT/CFP Operating Procedures should also be followed for the ultimate beneficial owners of bodies corporate or legal arrangements who are confirmed to be PEPs, as well as for the existing client base to ensure that all current PEPs have been so identified and remain subject to

---

84 Division Chief, Banking and Currency Operations Division
85 POC (MLP) Regulations, r. 7(1)(c); TP(RE) Regulations, r 5(1)(b)
86 POC(MLP) Regulations, Regulation 19; TP (RE) Regulations, r21
enhanced customer due diligence processes.

9.4.1. Correspondent Banking

a) Correspondent banking refers to the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). The arrangement is used by respondent banks (such as local DTIs) to conduct business and access services (such as cash management, international wire transfers, cheque clearing, payable through accounts and foreign exchange services), which the respondent banks cannot offer directly because of the lack of an international network.87

b) Countries are required by FATF to ensure financial institutions 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. In considering the establishment or maintenance of relationships, the Central Bank must have regard to the FATF requirements as well as to the matters reflected in the Risk Assessment Guide in this document at paragraph 6 above. Regard must also be had of the Wolfsberg Group88 updates on correspondent banking guidelines.

c) The Note on USA Financial Institutions Offering Correspondent Banking

87 Basel Committee on Banking Supervision- Sound Management of Risks Related to ML and TF, January 2014 – Appendix 2-general considerations on correspondent banking
88 The Wolfsberg Group is an association of thirteen global banks which aims to develop frameworks and guidance for the management of financial crime risks, particularly with respect to Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies. The Group came together in 2000, at the Château Wolfsberg in north-eastern Switzerland, in the company of representatives from Transparency International, including Stanley Morris, and Professor Mark Pieth of the University of Basel, to work on drafting anti-money laundering guidelines for Private Banking. The Wolfsberg Anti-Money Laundering (AML) Principles for Private Banking were subsequently published in October 2000, revised in May 2002 and again most recently in June 2012. Source: www.wolfsberg-principles.com/about/mission.

The Wolfsberg Group consists of the following financial institutions: Banco Santander, Bank of Tokyo-Mitsubishi-UFJ Ltd, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JPMorgan Chase, Société Générale and UBS. Source: Wolfsberg Group Principles on Correspondent Banking.
Banking Services 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 state89. 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 agreement90.

---

89 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

90 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
d) While the Central Bank 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 requisite measures are engaged vis-à-vis such relationships. If the Central Bank took a decision to provide correspondent banking services to foreign counterparts, the operating due diligence requirements should be guided by the matters reflected in the BOJ AML/CFT/CFP Guidance Notes91 to the industry on correspondent banking as well as considerations such as -

i. SWIFT membership;

ii. Regulatory status including whether there is a licence to undertake the banking and/or securities business;

iii. Adequacy of AML, CFT and CFP controls;

iv. Stock Exchange listing in G10 country or in approved CARICOM State.

e) Additionally, the Central Bank must 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:

i. whether the respondent bank permits “payable through accounts”. This would be one foreseeable way in which shell banks could take advantage of respondent banks;

ii. the country in which the foreign respondent bank resides; (see BOJ AML/CFT/CFP Guidance Notes92 on countries with inadequate AML/CFT/CFP 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.

9.4.2. 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 and other due diligence procedures and risk assessment and risk mitigation measures set out in this policy.

9.4.3. Wire Transfers and Other Electronic Funds Transfer Activities

a) The interpretive note to FATF Recommendation 16\(^{93}\) defines the term 'wire transfer' to 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. For all wire transfers or electronic funds transfers, whether domestic or cross border, refer to Regulation 9 of the POC(MLP) Regulations and Regulation 9 of the TP (Reporting Entities) Regulations to see the information that should be obtained and retained. Section 10 of the BOJ AML/CFT/CFP Operating Procedures outlines information that should be obtained and retained for the period stated in the AML/CFT/CFP Regulations\(^ {94}\) when conducting any/all electronic fund transfers (wire transfers, remittances etc.).

\(^{93}\) Glossary of specific terms used in R16 (Wire transfers)
\(^{94}\) Regulation 9 of the POC(MLP) Regulations and regulation 9 of the TP (Reporting Entities) Regulations
(i) 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 “Requirements for signature”) should be borne in mind.

**9.4.4. Transferring Customers**

Where accounts are transferred from a 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.

**9.4.5. Non-Face-to-Face Customers**

Transactions being conducted by a customer on behalf of another customer or a third party should be subject to more rigorous verification and identification standards and stringent due diligence measures including where necessary or deemed appropriate in the circumstances, approval by the Director Banking Department and the Division Chief, Banking and Currency Operations Division.

**9.4.6. Data Protection**

a) In 2020 Jamaica passed The Data Protection Act (“DPA”) which will impact the Central Bank’s operations. The objectives of this Act are to -
i. define the general principles for the treatment of “personal data” relating to an individual;

ii. strengthen the protection of personal data, and

iii. provide for oversight of the treatment of personal data in a manner that is transparent and which will enable the repositories of personal data (“data controllers”) to strengthen the protection of personal data.

b) When the DPA takes effect, the data protection obligations will be applicable to:-

i. The public and private sectors in Jamaica as well as the Parliament. Data controllers include public authorities, defined to include a Ministry, Department or Executive Agency or other agency of Government); and

ii. Persons not established in Jamaica but who use equipment in Jamaica for processing personal data otherwise than for the purpose of transit through Jamaica (i.e. possibly call-centre type of services or processing centres or ‘business hubs’ as against information transmitted via electronic fund transfers en route to another jurisdiction)

c) Bank of Jamaica falls within the definition of a “data controller” under the DPA to the extent that the Central Bank *inter alia* processes *personal data* pursuant to statutory functions under the statutes that it administers. Thus, the Central Bank, as a data controller, will be required to adhere to the DPA when this becomes law.

d) The Central Bank also does business with customers who are nationals or citizens (including Embassy personnel) of jurisdictions with Data Protection legislation such as the EU territories, customers such as those purchasing souvenir coins and those who conduct
over the counter transactions to redeem foreign currency. The Central Bank also has correspondent banking relationships with banks in the EU.\(^5\)

### 10. INSTITUTIONAL ARRANGEMENTS – MAINTENANCE AND UPDATING OF THE POLICY

10.1. In order to maintain its relevance, there shall be ongoing review of the Policy by the Nominated Officer in conjunction with the Legal Department. All proposed amendments will be submitted to the Senior Nominated Officer for review prior to obtaining approval from the Deputy Governor, Banking and Currency Operations & Financial Market Infrastructure Divisions and the endorsement by the Management Council. Following the endorsement by the Management Council and subsequent approval by the Bank’s Board of Directors, the revised Policy will be published on the Bank’s website.

10.2. The Policy must be reviewed at least once every 24 months.

10.3. In addition to the mandatory frequency outlined above, a review of the Policy is triggered once there are changes to the applicable local legislation and international best practices principles and international standards such as FATF 40 Recommendations.

10.4. Procedures for updating /effecting amendments to the Policy

The review must be conducted as follows:

a) Periodic review by the Banking Department in conjunction with the Legal Department,

---

\(^5\) The General Data Protection Regulations (GDPR) apply to each member state of the EU aiming to create more consistent protection of the consumer and personal data across EU member states. It mandates for a set of standards to be created by companies that handle EU citizens’ data to better safeguard the processing and movement of citizens. The Regulation applies to personal data of the natural person or “data subject” that can be used directly or indirectly. The GDPR also applies to all organizations holding and processing EU resident’s personal data, regardless of geographic location and further dictates that data controllers and processors GDPR applies to data controllers and processors established outside the EU and offer goods and services to data subjects who are within the EU whether or not for a fee.
b) Submit draft document to Division Chief, Banking & Currency Operations Division for review and sign off

c) Division Chief, BCOD, submits updated document to the Deputy Governor, BCOD&FMID for approval. The document is then submitted to the Board for approval.

d) Upon Board approval, the Policy is published on the Bank’s website at (www.boj.org.jm).
Money Laundering

The term ‘money laundering’ refers to all procedures, methods, and transactions designed to change or disguise the source or identity of illegally obtained money so that it appears to have originated from a legitimate source\. Under the Proceeds of Crime Act (‘POCA’) money laundering is any activity amounting to dealings with criminal property or the proceeds thereof\. Criminal property is any property that constitutes a benefit derived wholly or partially from criminal conduct. Criminal conduct means any conduct constituting an offence in Jamaica, or if outside, conduct that would constitute a crime in Jamaica. (See also paragraphs 18-21 of the BOJ AML/CFT/CFP Guidance Notes (Revised) 2018)

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 sufficient if it can be proven that there was willful 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 be aware that under the POCA the predicate offences (i.e. offences from which a money laundering charge can be derived) include any serious offence. Once therefore an offence is committed, if criminal property is involved or a benefit has been derived from the commission or facilitation of that offence it is possible that charges of money laundering may also be brought in such circumstances. Charges in respect of offences involving for example breaches of intellectual property rights, or breaches of the relevant financial statutes, may

---

\(^{96}\) Taken from the BOJ AML/CFT/CFP Guidance Notes (Revised 2018)

\(^{97}\) See the POCA section 91(1)

\(^{98}\) See the POCA section 2
therefore possibly lead to additional charges of money laundering.

Criminal Lifestyle and Civil Forfeiture

The concepts of criminal lifestyle and civil forfeiture were introduced by the POCA.

1. 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 Parish 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 paragraphs 22 and 23 of the BOJ AML/CFT/CFP Guidance Notes (Revised 2018).)

2. 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).

3. Introduction of the civil forfeiture and criminal lifestyle regimes means that it is likely that financial institutions as well as the Central Bank will need to undertake enhanced due diligence or KYC measures to ensure that they are not in fact holding forfeitable assets\(^{100}\). 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

---


\(^{100}\) See POCA sections 6, s.5 (1), (2), (4), (13) & (14)
business of the customer or knowing the nature of the customer’s business; and source of wealth and source of funds checks and verification.

4. The civil forfeiture and criminal lifestyle regimes will be subject to third party interests where genuine cases are established. Under the POCA, third party interests will have to apply to the court for an order under sub-sections (12) and (13) of section 5 of the POCA re: Criminal lifestyle regimes. (See also POCA section 8. In relation to the civil forfeiture regime under POCA, third party interests are matters for the court’s consideration of an application for a civil recovery order (see sub-sections (4) and (5) of section 58 of the POCA. This means additional costs may be incurred by a financial institution to, for example, protect its interest in forfeitable property that it holds as collateral.

5. The offences to which the criminal lifestyle regime applies can be found in the Second Schedule to the POCA (i.e. drug trafficking, money laundering, murder, kidnapping, arms trafficking, forgery, infringements of intellectual property rights, larceny offences of obtaining credit by fraud and receiving stolen property, offence of conspiracy to defraud, embezzlement, extortion, terrorism offences, cybercrimes, child pornography, offences under the Sexual Offences Act, offences under the Law Reform (Fraudulent Transactions) Special Provisions Act (o/c “lottery scamming” legislation), offences under section 14(1)&(5) of the Corruption Prevention Act and an offence under section 4 of the Trafficking in Persons (Prevention, Suppression and Punishment) Act and inchoate offences (conspiracy, aiding, abetting, counseling etc.).

**Terrorist Financing**

Terrorist financing refers to financing of terrorist acts and of terrorists and terrorist organizations. Thus, under the Terrorism Prevention Act (“TPA”) the accommodating or facilitating of financial transactions that may be directly or indirectly related to terrorists, terrorist activities and/or terrorist organizations is an offence. Once the financial institution knows or suspects, or should reasonably

---

101 FATF Glossary (October 2020 page 129)
suspect that an individual or 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 (See also paragraphs 31-38 of the BOJ AML/CFT/CFP Guidance Notes (Revised 2018).


1. The United Nations Security Council Resolution Implementation Act (“UNSCRIA”) was passed in November 2013 and is designed for Jamaica to achieve compliance with Recommendation 7 (on targeted financial sanctions related to the prevention of the proliferation of weapons of mass destruction) of the revised FATF Forty Recommendations, 2012. The UNSCRIA is an enabling legislation which forms the basis for Jamaica to respond to directives or resolutions issued by the United Nations Security Council by promulgation of the requisite Regulations under this Act.

2. The UNSEC Resolutions Implementation (Asset Freeze - Democratic People’s Republic of Korea) Regulations, 2013 were issued pursuant to section 3 of the Act and these Regulations outline Jamaica’s mandates in relation to the directives of the UNSEC regarding the Democratic People’s Republic of Korea (DPRK) in Resolutions 1718(2006) and successor resolutions 1874(2009) and 2087(2013). These resolutions represent UN required sanctions comprising financial prohibitions to prevent the provision of financial services, financial resources or financial assistance to the DPRK (See also paragraphs 52-56 of the BOJ AML/CFT/CFP Guidance Notes (Revised) 2018.

3. The UNSCRA was amended in 2019 to, among other things, incorporate a listing mechanism for proscribed entities (similar to the Section 14 listed entity approach under the TPA. There is now also a mechanism for de-listing

102 Schedule to The UNSEC Resolutions Implementation Act, 2013
applications to be done by a proscribed entity.

4. Regulations under the UNSCRIA entitled the United Nations Security Council Resolution Implementation (Reporting Entities) Regulations, were promulgated in November 2019. These regulations, among other things, outline the regime by which institutions under the UNSCRIA can comply with their reporting obligations; and establishes the concept, role and functions of the Competent Authority under the UNSCRIA.
Appendix II

FATCA

1. Jamaica signed the IGA Reciprocal agreement with the USA on May 01, 2014 pursuant to the Foreign Account Tax Compliance Act (FATCA).

2. FATCA framework requires specific legislation be implemented in Contracting States to give legal effect to the FATCA agreement. Accordingly, amendments to the Revenue Administration Act\textsuperscript{103} were effected in August 2015 with the objective of complying with the FATCA.

3. Reporting obligations are detailed in the Regulations, 2015 to the RAA which are set out in the Second Schedule to the RAA. Reporting obligations pursuant to the RAA arise in relation to the calendar year 2014 and onwards.

4. BOJ as the Central Bank, would fall under Paragraph I.C. of Annex II of the IGA: \textit{Exempt Beneficial Owners other than Funds}. The following Entities shall be treated as Non-Reporting Jamaican Financial Institutions and as exempt beneficial owners for purposes of sections 1471 and 1472 of the U.S. Internal Revenue Code, \textit{other than} with respect to a payment that is derived from an obligation held in connection with a commercial financial activity of a type engaged in by a Specified Insurance Company, Custodial Institution, or Depository Institution.

5. \textbf{Central Bank} An institution that is by law or government sanction the principal authority, other than the government of Jamaica itself, issuing instruments intended to circulate as currency. Such an institution may include an instrumentality that is separate from the government of Jamaica, whether or not owned in whole or in part by Jamaica.

 BOJ would therefore be treated as a Non-Reporting Jamaican Financial Institution and as exempt beneficial owners for the purposes of sections 1471

\textsuperscript{103}In 2020 the RAA was amended to allow Jamaica to ratify the Convention on the Mutual Administrative Assistance in Tax Matters, to which Jamaica became a signatory in 2018. Administrative Assistance under this Convention means – Exchange of information; assistance in recovery and service of documents. As a central bank BOJ is excluded from the definition of a “reportable jurisdiction person” under this regime.
and 1472 of the U.S. Internal Revenue Code (subject to the commercial financial activity exception). This means that BOJ would be exempt from reporting obligations under FATCA subject to the commercial financial activity exception indicated in the Code).
Appendix III

Applicable Extracts from the Human Resource (HR) Policy Manual

The applicable extracts are as follows:

**Human Resources Policy Manual (Extract)**

i. **Section 8** (paragraph 8.3) A member of staff shall not seek to profit financially or otherwise, by making use of information acquired directly or indirectly in the course of his/her duties.

ii. **Section 10 – Disclosure of Personal Interest – Conflict of Interest**
   10.1 If in the course of duty, a member of staff is called upon to deal with any matter in which he/she has or may have a personal interest, such interest shall be immediately disclosed to the Head of the employee’s department, or, where the issue involves the Department Head, to the Governor.

iii. **Section 11 – Alteration and Falsification of Records**
   11.1. No unauthorized erasures and alterations are to be made in any of the Bank’s books or records.
   
   11.2. All internal erasures and alterations are to receive authorization from the immediate supervisor.
   
   11.3. No falsification is to be made to the Bank’s records.

iv. **Section 12 – Duty to Report Fraud**
   Each employee has a duty to report to the Head of his/her Department or to the Governor, any dishonest practices on the part of a colleague, which may come to his/her knowledge.

v. **Section 13 – Gratuity or Gifts from the Public**
   A member of staff is prohibited from accepting either for himself/herself or a family member, any fee, gift, gratuity or
consideration whatsoever, in connection with a service rendered in the employee’s official capacity.

vi. **Statutory Asset Declaration**
Staff members above a certain income bracket are also subject to statutory declaration requirements under the Integrity Commission Act and the Bank has implemented a monitoring mechanism to monitor compliance with this law\(^{104}\).

---

\(^{104}\) The Integrity Commission Act ("ICA"), came into operation on 22 February 2018. This Act repealed the statutory declaration obligation for public servants/officers that were set out in the Corruption Prevention Act and the related declaration form and relocated those obligations under the ICA and introduced a revised statutory declaration form. The reporting periods and timeline remain the same under the ICA.

Employees who earn above JMD3.5million are also subject to the statutory annual asset declaration requirements of the Integrity Commission Act;
### Appendix IV

**The Proceeds of Crime (Money Laundering Prevention) Regulations**

**Schedule - Form I**

<table>
<thead>
<tr>
<th>Part 1: Reporting Financial Institution Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Name of Financial Institution</td>
</tr>
<tr>
<td>2. Address of Financial Institution</td>
</tr>
<tr>
<td>3. TRN.</td>
</tr>
<tr>
<td>4. Branch address</td>
</tr>
<tr>
<td>5. Type of Financial Institution</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 2: Person(s) involved in Transaction(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section A: Persons on whose behalf Transaction is conducted (Customer)</td>
</tr>
<tr>
<td>6. Multiple persons [ ]</td>
</tr>
<tr>
<td>7. Individual's last name or organization's name</td>
</tr>
<tr>
<td>8. First name</td>
</tr>
<tr>
<td>9. M.I.</td>
</tr>
<tr>
<td>10. Permanent Address</td>
</tr>
<tr>
<td>11. Date of Birth (DD/MM/YYYY)</td>
</tr>
<tr>
<td>12. TRN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 3: Method used to verify identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>13. [ ] Examined identification credential/document</td>
</tr>
<tr>
<td>[ ] Known Customer – Information on file</td>
</tr>
<tr>
<td>14. Describe identification credential: a. [ ] Driver's licence</td>
</tr>
<tr>
<td>e. issued by: f. Number:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 4: Occupation/Business/Principal Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>15. [ ]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 5: Person(s) conducting transaction (Agent)</th>
</tr>
</thead>
<tbody>
<tr>
<td>17. Multiple persons [ ] See Part 6</td>
</tr>
<tr>
<td>18. Individual's last name or organization's name</td>
</tr>
<tr>
<td>19. First Name</td>
</tr>
<tr>
<td>20. M.I.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 6: Method used to verify identity</th>
</tr>
</thead>
<tbody>
<tr>
<td>21. [ ] Examined Identification credential/document</td>
</tr>
<tr>
<td>[ ] Known Customer – Information on file</td>
</tr>
<tr>
<td>22. Date of Birth (DD/MM/YYYY)</td>
</tr>
<tr>
<td>23. TRN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 7: Person(s) benefiting from transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>26. Multiple persons [ ] See Part 6</td>
</tr>
<tr>
<td>27. Individual's last name or organization's name</td>
</tr>
<tr>
<td>28. First Name</td>
</tr>
<tr>
<td>29. M.I.</td>
</tr>
</tbody>
</table>
### The Proceeds of Crime (Money Laundering Prevention) Regulations, 2007

**PART 3  Preparer Information**

<table>
<thead>
<tr>
<th>31. Last Name</th>
<th>32. First Name</th>
<th>33. M.I.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>34. Title</th>
<th>35. Phone No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>36. Signature</th>
<th>37. Date of Signature (DD/MM/YYYY)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PART 4  Contact for Assistance (if different than prepare info. in Part 3)**

<table>
<thead>
<tr>
<th>38. Last Name</th>
<th>39. First Name</th>
<th>40. M.I.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>41. Title</th>
<th>42. Phone No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**PART 5  Transaction Details**

<table>
<thead>
<tr>
<th>2. Transaction Type</th>
<th>3. Date (DD/MM/YYYY)</th>
<th>4. Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>5. Transaction Currency</th>
<th>6. Transaction Account</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7. Accounts Affected (if any)</th>
<th>8. JAS Equivalent</th>
<th>9. JAS Exchange Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Number</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>10. USS Equivalent</th>
<th>11. USS Exchange Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>12. Source of funds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>13. Transaction Type</th>
<th>14. Date (DD/MM/YYYY)</th>
<th>15. Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>16. Transaction Currency</th>
<th>17. Transaction Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>18. Accounts Affected (if any)</th>
<th>19. JAS Equivalent</th>
<th>20. JAS Exchange Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Number</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>21. USS Equivalent</th>
<th>22. USS Exchange Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>23. Source of funds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>24. Transaction Type</th>
<th>25. Date (DD/MM/YYYY)</th>
<th>26. Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>27. Transaction Currency</th>
<th>28. Transaction Account</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Affected</td>
<td>J$ Equivalent</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Type</td>
<td>Number</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>USS Equivalent</th>
<th>USS Exchange Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source of funds</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transaction Type</th>
<th>Date (DD/MM/YYYY)</th>
<th>Time</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Transaction Currency</th>
<th>Transaction Account</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Account Affected</th>
<th>J$ Equivalent</th>
<th>J$ Exchange Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Number</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>USS Equivalent</th>
<th>USS Exchange Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source of funds</td>
<td></td>
</tr>
</tbody>
</table>

**PART 6**
Reason for Suspicion
Appendix V
Examples of Unusual/Suspicious Activities

Provision of Insufficient or Suspicious Information.

1. Cash Transactions

    a) Cash deposits which are not consistent with the business activities of the customer.

    b) Increases in cash deposits of the customer 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.

    c) Unusually large cash deposits by a customer whose ostensible business activities would normally be generated by cheques and other instruments.

    d) Cash deposits by a customer, by means of numerous credit slips so that the total of each deposit is unremarkable, but the total of all the credits is significant.

    e) Requests for the exchange of large quantities of low denomination notes for those of higher denomination.

    f) The transfer by a customer of large sums of money to or from overseas locations with instructions for payment in cash.

    g) Frequent exchange of cash into other currencies.

    h) The constant pay-in or deposit of cash by a customer to cover requests for financial institutions’ drafts, money transfers or other negotiable and readily marketable money instruments.

    i) Large cash deposits using night depository facilities, thereby avoiding direct contact with financial institution staff.

105 Bank of Jamaica Guidance Notes on the Prevention of Money Laundering and Countering the Financing of Terrorism, Proliferation and Managing Related Risks, 2018 – Appendix V.
j) Company accounts whose deposits and withdrawals are by cash rather than the forms of debit and credit normally associated with commercial operations (for example, cheques, Letters of Credit, Bills of Exchange, etc.) or in relation to which withdrawals are made therefrom and requests made for payment into personal accounts.

k) 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;

2. Operation of Accounts

a) The use of a number of trustee or clients' accounts which do not appear consistent with the customer's type of business, including transactions which involve nominee names.

b) Increases in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts especially if the deposits are promptly transferred between other client company and trust accounts.

c) Large number of individuals making payments into the same account without an adequate explanation.

d) Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.

e) Matching of payments out with credits paid in by cash on the same or previous day.

f) Paying in large third-party cheques endorsed in favour of the customer.
g) High account turnover inconsistent with the size of the balance (suggesting that funds are being “washed” through the account).

h) 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.

i) See k) in cash transactions above

3. Additional Considerations for Transactions Involving Terrorist Financing

a) Accounts that receive relevant periodic deposits and are dormant at other periods;

b) A dormant account with a minimal sum suddenly receiving a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed;

c) Customer refuses to provide information required by financial institution, or attempts to reduce the level of information provided or to provide information that is misleading or difficult to verify;

4. Investment Related Transaction

a) 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.

b) Buying and selling of a security with no discernible purpose or in circumstances which appear unusual.

c) Requests by customers for investment management services (either foreign currency or securities) where the source of the funds is unclear or not consistent with the customers’ apparent standing.
5. Off-Shore International Activity
   a) Building up of large balances, not consistent with the known turnover of the customer's business, and subsequent transfer to account(s) held overseas.
   b) Use of Letters of Credit and other methods of trade finance to move money between countries where such trade is not consistent with the customer's usual business.
   c) Regular and large payments by customers, including wire transactions, that cannot be clearly identified as bona fide transactions to, or receipt of regular and large payments from, countries which are commonly associated with the production, processing or marketing of drugs or money laundering, or which are regarded as tax havens.
   d) Unexplained electronic fund transfers by customers on an in-and-out basis and without passing through an account.

6. Secured and Unsecured Lending
   a) Customers who repay problem loans unexpectedly.
   b) Requests to borrow against assets held by the financial institution or a third Party, where the origin of the assets is not known or the assets are inconsistent with the customer's standing.
   c) Requests by customers for a financial institution to provide or arrange financing where the source of the customer's financial contribution to the transaction is unclear, particularly where property is involved.
   d) Requests for loans to offshore companies, or loans secured by obligations of offshore financial institutions.
   e) Customers purchasing certificates of deposit and using them as loan collateral.
7. Overseas correspondents and other foreign counterparts seeking to conduct business from jurisdictions that are currently on FATF’s list of High Risk jurisdictions; and

Overseas correspondents and other foreign counterparts 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 (e.g. special purpose vehicle (s.p.v.); or trustee; etc.)

8. 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.

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

10. 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.)
Appendix VI

Some of the Offences under the Required Disclosure Regime Under the POCA

1. **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 e.g. 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 not exceeding five (5) years, in the case of a body corporate, a fine not exceeding $5million.

2. **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.

3. **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.

4. **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 $1 million 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.
Appendix VII

Some of the Financing of Terrorism Offences under the TPA

1. The TPA was passed in 2005, and amended in 2010, 2011, 2013 and 2019. The Act outlines the activities listed in this appendix as financing offences.

2. Terrorist/Terrorism Financing Offences

   (a) Directly or indirectly, wilfully and without lawful justification or excuse collecting property, providing or inviting a person to provide, or make available property or other related services, -

      (i) intending that they be used, or knowing that they will be used in whole or in part -

          for the purpose of facilitating or carrying out terrorist activity;

          for the benefit of any entity known to be committing or facilitating any terrorist activity;

      (ii) knowing, that in whole or in part, they will be used by or will benefit a terrorist group (Section 4);

   (b) Facilitating or carrying out a terrorist activity by -

      (i) using property directly or indirectly, in whole or in part; or

      (ii) possessing property intending that it be so used or knowing that it will be so used directly or indirectly in whole or in part (Section 5);

   (c) Dealing directly or indirectly in or with any property that is owned or controlled by or on behalf of a terrorist group;

   (d) Entering into or facilitating, directly or indirectly, any transaction in respect of property owned or controlled by or on behalf of a terrorist group;
(e) Providing any financial or other related services in respect of that property for the benefit of or at the direction of a terrorist group;

(f) Converting any such property or taking any steps to conceal or disguise the fact that the property is owned or controlled by or on behalf of a terrorist group. (Section 6).

(g) The TPA states that a person who commits any of these listed offences, is liable on conviction in the case of an individual, to life imprisonment, and in the case of a body corporate, to a fine.

3. The TPA defines the following terms in Section 2:-

(a) ‘Applicable property’ – means any property (wherever situated) derived, obtained or realized, directly or indirectly from the commission of a terrorism offence or that has been used, in whole or in part, to facilitate or carry out a terrorism offence, whether in the hands of the offender or the recipient of a tainted gift. Specific rules have been set out to allow for identification of applicable property106.

(i) in which an interest is held - this constitutes property held by a person or property vested in a person as trustee in bankruptcy or liquidator;

(ii) in which an interest is obtained – constitutes property obtained by a person; and in relation to property comprising land, this includes an interest involving any legal estate or equitable interest or power. In relation to property other than land, this includes a ‘right’ (such as a right to possession);

(iii) in which an interest is transferred or granted – this constitutes property transferred to a person;

---

106 TPA Sections 2(2)-(7)
(iv) in which a person is beneficially interested or in which a person would be beneficially interested if the property was not vested in another as trustee in bankruptcy or liquidator;

This definition was revised to ensure that property held by designated persons; terrorist organizations and other supporters of terrorism, by themselves or jointly with third parties, wherever situated, would be subject to the tracking and enforcement mechanisms;

(b) ‘terrorism offence’ and ‘terrorist activity’ to include conspiracies, or attempting to commit, aiding, abetting, procuring or counselling activities;

(c) ‘tainted gift’ where an offender transfers property to another person for consideration which is significantly less than the value of the property. That property will constitute a tainted gift and the benefit gleaned will be calculated as the difference between the property value at the time of the transfer and the consideration.\footnote{107}

Property that can be traced in this regard will either be property given to the recipient and being held by the recipient; or any property in the recipient’s hands which directly or indirectly represents the property given; or property given to and held by the recipient and any property in the recipient’s hands which directly or indirectly represents the other part of the property given.

\footnote{107 Terrorism Prevention (Amendment) Act 2013 First Schedule (section 2)}
8. Requirements for signature.

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;
   
   c) of an encrypted signature or other method of indicating identity and approval;
   
   d) adduce evidence of the unreliability of an encrypted signature.
3. 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.

4. 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.

5. 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."