(2016)
GUIDANCE NOTES
ON
THE DETECTION AND PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING ACTIVITIES (AML/CFT)

This publication of the draft Guidance Notes for Consultation is available on the Bank of Jamaica's website www.boj.org.jm

Second Reissue April 2016

(Revised June 2005, March 2007, June 2007 and March 2009)

Initial Reissue August 2004

1st Update February 2005

2nd Update March 2005

3rd Update June 2005

4th Update March 2007

5th Update March 2009

Contents

Comments on this proposal should be submitted by 30 June 2016 by e-mail to: Maurene.Simms@boj.org.jm or FISDfeedback@boj.org.jm.

Alternatively, comments may be sent via post to:

Miss Maurene A. Simms
Division Chief
Financial Institutions Supervisory Division
Bank of Jamaica
Nethersole Place,
Kingston

GLOSSARY

BSA	-	Banking Services Act
BOJA	-	Bank of Jamaica Act
BOJ/the Bank	-	Bank of Jamaica
CDD	-	Customer Due Diligence
CTD	-	Chief Technical Director
DPP	-	Director of Public Prosecutions
FID	-	Financial Investigations Division
FI	-	Financial Institution
FSC	-	Financial Services Commission
FT	-	Financing of Terrorism
IOSCO	-	International Organization of Securities Commissions
JMD	-	Jamaican Dollars
KYC	-	Know Your Customer
MFAFT	-	Ministry of Foreign Affairs & Foreign Trade
ML	-	Money Laundering
MOFP	-	Ministry of Finance and Planning
POCA	-	Proceeds of Crime Act
POC (MLP) Regulations	-	Proceeds of Crime (Money Laundering Prevention) Regulations
STR	-	Suspicious Transaction Report
TF	-	Terrorism Financing
TPA	-	Terrorism Prevention Act
TPR/TP (Rep..Ent.) Regs.	-	Terrorism Prevention (Reporting Entities) Regulations
TTR	-	Threshold Transaction Report
UNSCRIA	-	United Nations Security Council Resolution Implementation Act
USD	-	United States Dollars

FOREWORD

These Guidance Notes have been substantially revamped and updated to take account of the amendments to the AML/CFT laws in Jamaica, the passage of the United Nations Security Council Resolutions Implementation Act, the revised FATF 40 Recommendations and revised FATF Guidance on matters covered in the FATF Recommendations.

Accordingly, the Guidance Notes seeks to encourage financial institutions (as defined herein) to apply a risk based approach to their respective AML/CFT policies and procedures; outlines the regulatory expectations in relation to the matter of scenarios classified as high risk and low risk; expands discussion on the KYC and CDD considerations; provides additional guidance on the matter of agent banking and responsibilities for group wide AML/CFT approaches, incorporates discussions on emerging issues such as the cash transaction limit requirements of the POCA; refocused approach to PEPs; the phenomenon of virtual currencies and highlights obligations which will attract sanctions on the AML/CFT Rules that will be issued under the Banking Services Act and Bank of Jamaica Act.

This document has been significantly altered from the ***Guidance Notes on the detection and prevention of money laundering and terrorist financing*** ('Guidance Notes') last issued in 2009, this prevented the inclusion of a schedule detailing the changes made to the previous document, within the timeline that would allow for consultation to occur by end April 2016.

SECTION I – PRELIMINARY PROVISIONS APPLICABILITY AND LEGAL STATUS OF THESE GUIDANCE NOTES

PRELIMINARY PROVISIONS

Interpretation

1.

"applicable legislation" means –

The Proceeds of Crime Act (POCA);

The Proceeds of Crime (Money Laundering Prevention) Regulations;

The Terrorism Prevention Act (TPA);

The Terrorism Prevention (Reporting Entities) Regulations;

The United Nations Security Council Resolution Implementation Act;

The United Nations Security Council Resolution Implementation (Asset Freeze – Democratic People's Republic of Korea) Regulations;

The United Nations Security Council Resolution Implementation Regulations (enacted from time to time);

The Charities Act;

The Revenue Administration Act;

The Financial Investigations Division Act;

The Banking Services Act;

The AML/CFT Rules (under the Banking Services Act and the Bank of Jamaica Act);

and all applicable amendments to these legislation up to the latest date of Guidance Notes reissue

"competent authority" has the meaning assigned :-

In the Proceeds of Crime Act ('POCA') competent authority is defined at section 91(g) for anti-money laundering purposes in relation to its functions set out at section 91A. In 2007, Bank of Jamaica was designated by the Minister of National Security, the competent authority for the financial institutions it regulates;

In the Terrorism Prevention Act ('TPA'), competent authority for counter financing of terrorism is defined at section 18(5) of the TPA. Bank of Jamaica undertook the role of competent authority until the formal designation was effected by way of letter dated 15th May, 2015 by the Minister of Finance and Planning;

"designated authority" means the Chief Technical Director of the Financial Investigations Division for the purposes of the POCA, TPA and the United Nations Security Council Resolution Implementation Act 2013;

"designated non-financial institution" has the meaning set out in the Fourth Schedule to the POCA ;

"financial institution' for the purposes of these Guidance Notes means a financial institution which falls under the AML/CFT jurisdiction of the Bank of Jamaica as follows -

(a) a financial holding company (as defined in the Banking Services Act ('BSA'))

(b) a commercial bank

(c) a merchant bank

(d) a building society

(e) a cooperative society carrying on business as a 'credit union'

(f) a person licensed under the Bank of Jamaica Act to operate an exchange bureau (i.e. a "cambio")

(g) a money transfer and remittance agent and agency as defined in section 2 of the Bank of Jamaica Act[1];

(h) any other financial institution which falls under the supervisory jurisdiction of the Bank of Jamaica;

"financial service" has the meaning assigned in the BSA;

Objective

2. These Guidance Notes have been issued pursuant to section 91(g)(ii) of the POCA and pursuant to Regulation 3 of the TP (Reporting Entities) Regulations. The objective of these Guidance Notes is to highlight to financial institutions that they are subject to the supervision of the Bank of Jamaica ('BOJ') (in its capacity as 'competent authority') as regards their responsibilities under the applicable legislation, as well as outline the best practices in the areas of Anti-Money Laundering ('AML') and Counter-Financing of Terrorism ('CFT') techniques.

[1] On 15 January 2002 Money Transfer and Remittance Agents and Agencies were designated financial institutions for the purposes of the Money Laundering Act by Ministerial Order. Subsequently on 12 February 2004, the BOJ Act was amended to formally establish the regulatory regime for money transfer and remittance agents and agencies and the requisite Operational Directions for these persons was issued on 5 July 2005.

These Guidance Notes will be reviewed periodically and amended as deemed necessary, to ensure their continued usefulness, efficacy, relevance and adherence to international best practice standards.

These Guidance Notes last revised in March 2009, were originally re-issued to the industry in August 2004 subsequent to initial circulation in this form in January and April of 2004. They therefore replaced the ones previously issued in August 2000 and the very first ones issued in July 1995.

APPLICABILITY OF THESE GUIDANCE NOTES

3. These Guidance Notes are informed by:-

(a) The FATF Revised Forty (40) Recommendations, 2012 (and related FATF generated Best Practice Papers);

(b) The Applicable Legislation (as defined in the interpretation section to these Guidance Notes) and

(c) Other AML/CFT related international requirements.

and apply to the financial institutions defined in these Guidance Notes and as discussed below in subparagraphs (i) and (ii).

(i) Agent Banking Services

Persons who obtain the authorization of BOJ to engage in agent banking services are subject to the requirements in these Guidance Notes and will also be subject to any AML/CFT Rules issued pursuant to the BSA. Each deposit taking institution is charged with the responsibility to ensure that their agent has adequate AML/ CFT controls policies and procedures in place for the permissible offering of banking services through the agent's operations.

Agents must ensure that their operations through which the banking services are provided are compliant with these Guidance Notes.

(ii) Retail Payment Service Providers

Persons who obtain authorization to offer retail payment services as outlined or defined in the "Guidelines for Retail Payment Services" issued by the BOJ will be expected to inform themselves of the requirements in these Guidance Notes in so far as the services or products offered will involve or require interfacing on any level with, or within, the operating space of a bank, merchant bank or building society.

LEGAL STATUS OF THESE GUIDANCE NOTES

4. Section 132(1) of the BSA and section 34F(6) of the BOJA give the BOJ the authority to make supervisory rules in relation to combatting money laundering, terrorism financing and the proliferation of weapons of mass destruction. These supervisory rules will mandate the compliance of licensees under the BSA and BOJA, with the mandatory obligations outlined in the BOJ Guidance Notes. This will allow for criminal or regulatory sanctions to be issued for non-compliance with the supervisory rules, as reflected in these Guidance Notes.

Mandatory Obligations

Mandatory obligations under these Guidance Notes, 2015 are set out in the areas pertaining to the subject matters itemized below on -

(a) Risk Based Framework - Section IV;

(b) Know Your Customer Requirements- Sections V;

(c) Nominated Officer Regime - Section VI;

(d) Governance Arrangements and Employee Integrity and Awareness - Section VII; and

(e) Internal Compliance Programme Requirements - Section VIII.

5. The AML/CFT laws[2] also reflect that in determining whether a person committed an offence under the POCA, or its Regulations or under the TPA or its Regulations, **a court**

[2] Section 94(7) of POCA and Regulation 2(3) of the POC (MLP) Regulations; TP(Reporting

shall consider any relevant supervisory or regulatory guidance issued by the Competent Authority which has jurisdiction over an entity which is charged with an offence under the POCA or under the (MLP) or (TP) regulations indicated. The Attorney General's Chambers has opined that the import and effect of this wording, is that it makes compliance with these Guidance Notes compulsory. Section 18(4) of the TPA further requires entities to consult with the Competent Authority for the purpose of carrying out their obligations to establish regulatory controls to enable them to fulfil their counter-financing of terrorism duties.

6. For a licensee under the BSA, a breach of its statutory obligations under the applicable legislation may be viewed as operating in a manner that constitutes unsafe or unsound practices for the purposes of paragraph 2 of Part A to the Fifth Schedule to the BSA. The ineffective or inadequate implementation of policies and procedures and controls is one possible example of a circumstance which may trigger enforcement under the BSA in this regard. (inadequate policies; inadequate assessment or analysis of risks; insufficient training sessions; inconsistent application of policies and procedures.)

7. If a licensee under the BSA is assessed to be operating in an unsafe or unsound manner, it can be subject to the following penalties under section 109 of the BSA–

    - Warning letter;
    - Voluntary Board Undertaking;
    - Supervisory directions; or
    - Cease and desist order

    Failure to comply with any such requirement, undertaking, direction or order constitutes an offence for which a person on conviction in a Resident Magistrate's court can be fined up to $5million and/or imprisoned for a term not exceeding one year.

8. In the case of Money Transfer and Remittance Agents and Agencies ("remittance companies") and Bureaux de Change ("cambios"), non-compliance with their respective AML/CFT obligations including these Guidance Notes, may result in the regulatory

Entities) Regulations, regulation 3.

sanctions, such as, being placed on probation and subject to enhanced monitoring or oversight, or the suspension or revocation of the licence.

9. A conviction for an offence under any of the applicable legislation can adversely impact a person's ability to be deemed as 'fit and proper' and to continue to operate within the sectors regulated by the BOJ.

10. Similar powers to take regulatory action for AML/CFT breaches will be applicable to credit unions when they become subject to regulation by the Bank of Jamaica. (Refer to paragraph 4 and 5 above) Additionally, credit unions should be aware that their level of compliance with the applicable legislation and these Guidance Notes will be amongst the matters considered in the review and assessment process for licence applications once the licensing regime has commenced. Currently where breaches of these Guidance Notes or the AML/CFT laws are identified in the operations of a credit union, both the credit union which is the subject of the breach, as well as the statutory regulator (i.e. The Registrar of Friendly and Cooperative Societies) are notified.

SECTION IA - BACKGROUND

MONEY LAUNDERING

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

It is recognized that cash lends anonymity to, and is therefore the normal medium of exchange for many forms of criminal activities, in particular, drug and arms trafficking, human trafficking, offences committed against persons (eg. murder/assassination/kidnapping), as well as criminal activities involving fraud, dishonesty and corruption (eg. tax evasion, extortion, infringement of copyrights or

dealings with illicit recordings). The extent and impact of these criminal activities globally have required countries to make concerted efforts to defend their institutions, financial systems, economies and citizens by criminalizing the proceeds of these crimes. Thus, in keeping with FATF Recommendation 3, POCA criminalizes any benefit derived directly or indirectly from any criminal conduct.

One of the most critical features of any AML regime is the protection of the financial system. Thus apart from ensuring that financial institutions do not commit the offence of money-laundering, they are placed under further statutory obligations to ensure that they take active, effective and ongoing steps to prevent and detect money laundering[3].

TERRORIST FINANCING

12. Terrorist financing refers to the act of accommodating or facilitating financial transactions that may be directly or indirectly related to terrorists, terrorist activities and/ or terrorist organizations. Once the financial institution knows or suspects or should reasonably suspect that an individual or group is associated with any terrorist activity or group, a financial institution (in carrying out a transaction for or with that individual or 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.

Financial institutions should also be aware, that business relationships with terrorists and terrorist organizations can expose the entity to significant legal, operational and reputation risks. These risks increase exponentially if the person or organization involved is later shown to have benefited from a lack of effective monitoring or wilful blindness on the part of the financial institution, and is found to have carried out, supported or facilitated acts of terrorism. Accordingly, financial institutions are placed under further statutory obligations to ensure that they take active, effective and ongoing

[3] See Regulation 5 of POCA (MLP) Regulations

steps to prevent and detect terrorist financing[4]. It may be difficult to detect funds linked to terrorist activities owing to the fact that terrorists or terrorist organizations often obtain financial support from legal sources. Other factors contributing to the difficulty of detection may also be the size and nature of transactions as these can be non-complex and in very small amounts.

Any financial institution that carries out transactions, knowing that the funds or property involved are owned or controlled by terrorists or terrorist organizations, or that the transaction is directly or indirectly linked to, or likely to be used in, terrorist activity, may be committing a criminal offence under the laws of many jurisdictions and such an offence in many instances may exist regardless of whether the assets involved in the transaction were the proceeds of the criminal activity or were derived from lawful activity but intended for use in support of terrorism. Additionally, some states have included in their legislation provisions intended to extend their local criminal jurisdiction beyond state borders. This is grounded on the premise that a person who commits a terrorist offence in a jurisdiction other than his own jurisdiction, can in fact be prosecuted by the local jurisdiction for the commission of a terrorism offence, so long as such offence if committed in the local jurisdiction would have been a terrorism offence. The TPA also provides that for the purpose of conferring jurisdiction, any offence committed outside of Jamaica will be deemed to have been committed in Jamaica where the offender may be domiciled for the time being in Jamaica, if such offence, when committed in Jamaica, would have been a terrorism offence[5].

13. A key issue for financial institutions therefore is to be able to identify any unusual and/or suspicious transaction that merits additional scrutiny and to record and report such transactions accordingly. In this regard, financial institutions should pay particular attention to: -

(a) The nature of the transaction itself;

(b) The parties involved in the transaction; and

[4] Section 18 TPA
[5] Section 46 TPA.

(c) The pattern of transactions or activities on an account over time.

See Appendix V, for examples of suspicious transactions which may be evidence of money laundering and/ or terrorist financing. Special attention must be given to elements of varying transactions which could indicate that the funds involved relate directly or indirectly to money laundering or terrorist financing. The list is not exhaustive and entities should be alert to evolving money laundering and/or terrorist financing techniques, patterns and typologies.

MUTUAL LEGAL ASSISTANCE

14. The United Nations Resolution 1373 and the revised FATF Recommendations (R.36-40) require that states must have the ability to provide mutual assistance to each other whether through the exchange of information, or facilitating the freezing and forfeiture of assets used to aid the commission of a terrorist offence in another jurisdiction. In Jamaica the Mutual Assistance (Criminal Matters) Act of 1995 and The Sharing of Forfeited Property Act of 1999, the Maritime (Drug Trafficking) Act, the Interception of Communications Act, and the Extradition Act permit Jamaica to extend assistance to other countries that are in the process of prosecuting, or enforcing judgments or forfeiture proceedings for a range of offences including drug related, revenue, money laundering and terrorist offences.

SECTION II – AML/CFT LEGISLATIVE AND REGULATORY FRAMEWORK – Applicable and other relevant legislation

{The following summaries do not constitute a legal interpretation of the sections of the Acts or Regulations referred to, and appropriate legal advice must be sought thereon}.

APPLICABLE LEGISLATION

THE PROCEEDS OF CRIME ACT (POCA)

15. POCA came into effect on 30 May 2007 and repealed and replaced the Money Laundering Act ('MLA') and the Drug Offences (Forfeiture of Proceeds) Act ('DOFPA').

POCA represents an all crimes approach to dealing with money laundering and generally the proceeds of crime. Money laundering is any activity amounting to dealings with criminal property[6]. Criminal property is any property that constitutes a benefit derived wholly or partially from criminal conduct. Criminal conduct[7] means any conduct constituting an offence in Jamaica, or if outside, conduct that would constitute a crime in Jamaica.

16. **POCA comprises seven parts as follows**:-

(a) **Part I** treats with the Assets Recovery Agency provisions. **Assets Recovery Agency** under section 3 means the Financial Investigation Division ('FID') of the Ministry of Finance and Public Service ('MOFP') or any other entity so designated by the Minister by Order. (See sections 2 and 3)

The Director under POCA means the Chief Technical Director ('CTD') of the FID or where another entity is designated, the person in charge of the operations of that entity. (See section 3(2))

[6] POCA section 91(1)
[7] POCA section 2

(b) **Parts II, III and IV** treat with enforcement and investigatory tools such as Forfeiture Orders, Pecuniary Penalty Orders and Restraint Orders, Disclosure Orders, Search and Seizure Warrants, Customer Information Warrants and Account Monitoring Orders and the criminal lifestyle regime. (See paragraph 20- 21 below for more details)

(c) **Part V** treats with the issue of money laundering, required disclosures, and offences under the POCA. **Under POCA, money laundering is any act which -**

(i) constitutes an offence under section 92 or 93; (See Section 91(1)(b)(i))

(ii) amounts to an attempt, conspiracy or incitement to commit an offence at section 92 or 93 of the POCA; (See Section 91(1)(b)(ii)) and

(iii) amounts to aiding, abetting, counselling, or procuring the commission of an offence under Section 92 or 93. (See Section 91(1)(b)(iii)).

(d) **Part VI** treats with offences under the POCA. The offences addressed under this aspect of the Act are in relation to investigations being conducted.

(e) **Part VII t**reats with matters general in nature such as regulation making powers under POCA, the repeal of the MLA and DOFPA and consequential amendments to other enactments.

Specific areas of concern under POCA Section V (Money Laundering) and under Section VI (Investigations) to Financial Institutions

17. **Offences under Section V (Money Laundering) are as follows:-**

(a) **Section 92** of the POCA, creates an offence where a person: -

(i) engages in a transaction that involves criminal property; **(section 92(1)(a));** or

(ii) conceals, disguises, disposes of, or brings into Jamaica, criminal property; **(section 92(1)(b));** or

(iii) converts or transfers or removes criminal property from Jamaica, **(section 92(1)(c)),** if that person knows or has reasonable grounds to believe at the time he does any act referred to at (a) (b) or (c), that the property is criminal property**. (Section 92(1))**

Financial institutions should note that 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 wilful blindness on the part of the person so charged. That is to say, it need only be proved that in the circumstances, it would have been reasonable for the person charged to believe or know that the property being dealt with was in fact criminal property.

Under the POCA, criminal property is property that constitutes a person's benefit (whether in whole, partially, directly or indirectly) from criminal conduct. It is immaterial who carried out or benefited from the conduct. **(Section 91(1)(a))**

(b) **Section 92(2)** of the POCA creates an offence where a person enters into or becomes involved in an arrangement that the person knows or has reasonable grounds to believe facilitates the acquisition, retention, use or control of criminal property by or on behalf of another.

Financial institutions should pay particular attention to this category of offence since this offence can be committed whether or not a transaction (in the traditional sense of the term), takes place. For instance, an offer of any kind or type of service, such as custodian or asset safe keeping services (e.g. safety deposit boxes) provided for property that is later viewed as criminal property; or the issue of letters of credit on behalf of persons who proceed to use these arrangements to acquire property which is later deemed to be criminal property both of these pose a significant risk to financial institutions and increases their exposure to prosecution and liability under POCA. Other services in respect of which caution should be applied include cheque cashing, arrangements

facilitating the movement of funds to accounts held (i.e. gift certificate arrangements); and changing out large bills to smaller bills or vice versa.

Financial institutions should ensure that their mandates with customers and contractual arrangements entered into in the course of the regulated business permit, the legal termination of the transaction, arrangement or business relationship if the institution conducting the transaction or facilitating the commercial arrangement form the view that criminal activity is taking place and to continue with the arrangement, relationship or transaction would expose that institution to legal or reputational risks due to the suspected criminal activity[8].

(c) **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.

(d) **Section 94(2)** makes it an offence for failing to make the requisite disclosure within the stipulated timeframe (i.e. within 15 days after the information or matter comes to a person's attention) (s. 94 (2)(c)) 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 (s. 94(2)(a)), and this knowledge or belief arose in the course of a business in the regulated sector (s.94(2)(c)); (Suspicious Transaction Report ('STR') obligation);

(e) **Section 95** makes it an offence where there is a 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)

[8] NCB v Olint - Privy Council Appeal No. 61 of 2008

(f) **Section 97** makes each of the following matters a 'tipping off' offence -

(i) Disclosing information with the knowledge or belief that a protected or authorized disclosure has been made under section 100, where such disclosure is likely to prejudice any investigation that might be conducted following the statutory disclosure. **(s. 97)(1)(a)**

Disclosures in this regard refer to disclosures by regulated businesses (via nominated officer regime) and disclosures to an authorized officer (refer to section 100(4)(a);

(ii) Disclosing information or any other matter with the knowledge or belief that the enforcing authority is acting or proposing to act in connection with a money laundering investigation that is being, or is about to be conducted **(s. 97(1)(b))**.

(g) **Section 101** makes it an offence for failing to make a report where cash (which includes bearer-negotiable instruments[9]) exceeding US$10,000 or the equivalent amount in any other currency, is being taken into or out of Jamaica **(s.101(2))**. The FID has introduced a standard reporting form which can be found on its website at www.fid.gov.jm.

18. **Offences under Section VI – Investigations are as follows:**

(a) Disclosing information or any other matter with the knowledge or belief that an investigation (whether regarding forfeiture; money laundering or civil recovery) is about to be or is being conducted. (section 104(2))

(b) Failure without reasonable excuse, to comply with a disclosure order (section 112);

[9] Section 101(1) POCA. In 2013 the penalty on conviction for an offence under section 101, was revised from J$10,000 to J$250,000 (refer section 12 of the POC (Amendment) Act, 2013.

(c) Failure by the financial institution without reasonable excuse, to comply with a customer information order (section 122(1);

(d) The financial institution making a statement that it knows is false or misleading in a material particular (section 122(3)(a));

(e) The financial institution recklessly making a statement that is materially false or misleading (section 122(3)(b)).

19. The responsibility for enforcing the provisions of the POCA is shared amongst the FID (in its capacity as the ARA and as designated authority through its CTD); the DPP; the Police; Customs; the Competent Authority, and any other person designated by the Minister. The responsibility for monitoring compliance with the obligations of the POCA is placed with the competent authority, which for financial institutions as defined in these Guidance Notes is the BOJ.

Areas of Enforcement Under POCA & POC (MLP) Regulations

Areas of Enforcement	**Section of Act/Regs.**	**Responsible Authority**	**Additional Information**
Threshold reporting	Reg. 3	CTD of the FID	
Required disclosure (STR)	Sections 94 & 100	CTD of the FID	
Account Monitoring Orders[10]	Section 126	ARA + (Constable; Officer designated by the Commissioner; Customs Officer; or any other	These persons are collectively referred to as the "Appropriate Officer".

[10] Section 126 of the POCA refers to an account monitoring order as an order directing a financial institution to give such information and documents as the Appropriate Officer requires in his application for this order. The order requires a financial institution to produce documents and/or information obtained by or that are under the control of the financial institution about transactions conducted through accounts held by a particular person with the financial institution.

		person designated by the Minister)	
Areas of Enforcement (cont'd…)	**Section of Act/Regs.**	**Responsible Authority**	**Additional Information**
AML Guidance & implementation of AML measures and monitoring compliance with the AML laws and guidance.	Sections 91 & 91A	Competent Authority	BOJ for licensees under the BSA, credit unions, cambios and remittance companies. FSC for non-DTIs (i.e. Securities dealers, Insurance Companies; Pension Funds Managers; Collective Investment Schemes). The Public Accountancy Board for Accountants; General Legal Council for Attorneys[11]; The Real Estate Board for Real Estate Dealers; The Betting, Gaming and Lotteries Commission for the gaming sector; The Casino Commission for casinos.
Forfeiture & Pecuniary Penalty Orders	5 – 32	ARA The DPP	
Restraint Orders	33	ARA The DPP	
Seizure of realizable property[12] that is subject to Restraint Order	36	A Constable Customs Officer An officer of the ARA/Agency	These persons are collectively referred to as "Authorized Officers"

[11] The regime for Attorneys is currently subject to an injunction and as such the Guidance developed by the GLC and AML/CFT Supervisory mandate of the GLC for Attorneys is not in effect.

[12] "Realizable property" is any free property held by the defendant for the purposes of the criminal lifestyle and civil forfeiture regimes; or any free property held by the recipient of a tainted gift.

		Any other person designated by the Minister	
Areas of Enforcement (cont'd…)	**Section of Act/Regs.**	**Responsible Authority**	**Additional Information**
Recovery Orders pursuant to the Civil Forfeiture Regime	57	ARA The DPP	
Disclosure Orders	105	Appropriate Officer	ARA + (Constable; Officer designated by the Commissioner; Customs Officer; any other person designated by the Minister)
Ancillary Orders	110	Appropriate Officer	
Search & Seizure Warrants	115	Appropriate Officer	
Customer Information Orders	119	Appropriate Officer	

20. The tools used for enforcement and investigation are Forfeiture Orders, Pecuniary Penalty Orders, Restraint Orders, Disclosure Orders, Search and Seizure Warrants, Customer Information Orders and Account Monitoring Orders.

(a) **A forfeiture order** is an order by the court that, in the case of a person's conviction for any offence in proceedings before the court, any property used in or in connection with the offence concerned be forfeited to the crown. A forfeiture order can also be made where the court determines that a person convicted for an offence has a criminal lifestyle and that person has benefited from his general criminal conduct. In this case the forfeiture order would be made in relation to the property identified as that person's benefit from his criminal conduct. (section 5)

(b) **A pecuniary penalty order** is an order by the court for the person against whom the order is issued, to pay to the Crown an amount equal to the value of the benefits derived by that

person from his/her criminal conduct. An order of this nature would usually be made in circumstances where the property representing the benefit from criminal conduct cannot be made subject to an order for forfeiture. (section 5(3)(b))

(c) **A restraint order** is an order by the court prohibiting any person from dealing with any realizable property held by a specified person. Realizable property means any property held by the person who is the subject of the order; or any free property held by the recipient of a tainted gift. (section 33 and section 2)

(d) **A search and seizure warrant** is a warrant authorizing:

(i) The entry and search of premises specified in the warrant; and

(ii) The seizure and retention of any information or material found which is likely to be of substantial value, whether by itself or not, to the investigation in respect of which the search warrant has been issued.(S. 115(3)).

The Act states that this warrant does not confer the right to seize any information or material in respect of which production can be refused on the grounds of legal professional privilege in proceedings in the Supreme Court. (Section 117)

(e) **A disclosure order** is an order by the court that requires the person on whom it is served to either produce or grant access to, information or material to an appropriate officer or answer questions at a place or time specified in the order (s.105(3)). **The Act states that this Order does not require production of or access to information that can be refused, that is, "excluded material" [13]or information or material that can be refused on the grounds of legal professional privilege in proceedings in the Supreme Court.**[14](See section 108)

[13] "Excluded material" per section 103 of POCA means:- (a) medical records; (b) human tissue or fluid which has been taken for the purpose of diagnosis or medical treatment and which a person holds in confidence.

[14] Legal privilege according to (Gilbert Law Summaries Dictionary of Legal Terms), is a person's privilege to refuse to disclose and to prevent others from disclosing anything said in confidence to that person's Attorney. Legal privilege applies to –

(f) **A customer information order** is an order by the court for information on whether a person holds/held (solely or jointly) any account with a financial institution or has conducted a transaction with a financial institution. Note the particular information required in the case of individuals -

(i) Account / transaction number;

(ii) Full name and date of birth;

(iii) TRN (see section V on KYC for further guidance):

(iv) Most recent address and previous addresses;

(v) Date on which the individual began to hold the account;

(vi) Date on which the individual ceased to hold the account;

(vii) Transaction date and description of transaction type;

(viii) Identity obtained by the financial institution;

(ix) Full name, date of birth, most recent and previous addresses of the joint holder of the account;

(x) Account number of any other accounts to which the individual is a signatory and details of the persons holding those accounts.

Note the Particular information required in the case of non-individuals-

1. Account number;
2. Entity's full name;
3. Description of the business carried on by the entity;
4. Country or jurisdiction of incorporation or establishment;

(i) matters that come within the ordinary scope of professional employment of an attorney and which are received in the attorney's professional capacity, either from a client or on the client's account, and for the client's benefit in the transaction of the client's business; or

(ii) communications from the client received by the attorney in the course of employment with the client and which relate to matters which the attorney becomes aware only through the professional relationship with the client. (See The Queen v. Cox and Railton – (1884) QBD 153 C.A.

For the purposes of Section V of the POCA, information comes to an Attorney in privileged circumstances where-

(i) it is given by the client directly or indirectly in connection his giving legal advice to the client;

(ii) it is given directly or indirectly by a person seeking legal advice; or

(iii) it is given by a person in connection with legal proceedings or contemplated legal proceedings. (s. 94(8))

5. TRN (see section V on KYC for further guidance);
6. Registered office or place of business (in or outside of Jamaica);
7. Date on which the entity began to hold the account;
8. Date on which the entity ceased to hold the account;
9. Evidence of the entity's identity obtained by the financial institution;
10. Full name, date of birth, most recent and previous addresses of any person who is a signatory to the account.

(g) **An Account Monitoring Order** is an order by the court to a financial institution to provide the account information specified in the order to an appropriate officer for the period and at or by the time or times specified in the order. For these purposes, account information means information relating to an account held at, or a transaction conducted with, the financial institution specified in the order, by the person specified in the order whether solely or jointly with another. (Sections 126(5) and (4)) **Under the POCA an accounting monitoring order has effect notwithstanding any restriction on the disclosure of information, however imposed** (Section 126(7)).

Criminal Lifestyle Principle

21. This concept of criminal lifestyle was introduced by POCA. Once a person has been convicted of any offence before the Supreme Court or has been committed to the Supreme Court from the RM Court pursuant to a determination on a forfeiture order or pecuniary penalty order, the Court at that point is required to make a determination on the issue of criminal lifestyle. (Section 5(1))

(a) Under the POCA a person shall be deemed as having a criminal lifestyle if –

(i) the person is convicted for an offence specified in the Second Schedule;

(ii) the offence for which he is convicted or committed (by an RM Court whilst in custody or on bail) constitutes conduct forming Section of a course of criminal activity, from which the person obtains a benefit; or

(iii) the offence for which he is convicted or committed (by an RM Court whilst in custody or on bail) committed over a period of at least one month and the person has benefitted from the conduct constituting the offence. (Section 6(1))

(b) A court's assessment of the determination of the "criminal lifestyle issue will look at-

(i) whether there is a criminal lifestyle and whether there has been some benefit from the general criminal conduct. If the determination is that there has been some benefit from criminal conduct, the court will then identify the property that represents that benefit, and either make an order for the property to be forfeited to the Crown; or make an order for the payment of an amount equal to the value of the benefit obtained; (section 5(3)).

(ii) if the determination at (a) is in the negative then the determination will be as to whether there has been any benefit from the particular criminal conduct (for which the person was convicted);

(iii) identification of any property used in or in connection with the offence concerned and make an order for same to be forfeited to the Crown;(section 5(2)).

(c) **Statutory safeguards to the above powers of forfeiture include the following:**

(i) In considering whether a forfeiture order should be made the Court must take into account –

- Third Party rights and interests in the property;
- The gravity of the offence concerned;
- Any hardship that might reasonably be expected to be caused by the order;
- The use that is ordinarily made of the property or the intended use of the property; (section 5(4))

(ii) Not less than 14 days written notice of an application for a forfeiture or pecuniary penalty order must be given by the enforcing authority to the Defendant and any other person it is believed to have an interest in the property targeted for forfeiture. Additionally, a copy of the notice must be published in a daily newspaper printed and circulated in Jamaica; (section 5(11)).

(iii) Persons claiming an interest in the property targeted for forfeiture may apply to the court for an order (section 5(12)) declaring the nature, extent and value of their interest in the property. Before such an order is made the court must first be satisfied that the applicant was not in any way involved in the commission of the offence; that the person acquired his interest for sufficient consideration and without knowing or having reasonable grounds to suspect that at the time the property was acquired, it was tainted property; (section 5(13)).

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

Civil Forfeiture Regime

22. POCA also allows for civil forfeiture

(a) The authorized officer[15] can take the following actions in respect of property constituting cash, which is not less than the statutory minimum[16] of J$100,000 and which is believed to be obtained directly or indirectly by or in return for or in connection with unlawful conduct:-

[15] Any of the following individuals may be considered an authorized officer- a constable, customs officer or the Minister's designate.
[16] POCA Section 55(1)

(i) Search of premises where it is believed cash is kept (section 72(1));

(ii) Search of a person or of any article in that person's possession whom it is believed is carrying cash (section 72(3)) ; (a person may be detained for as long as is required for the exercise of these powers – section 72(4));

(iii) Seizure of any cash (section 75) (initial detention period is 72 hours which period may be extended on application to a RM court (section 76);

(iv) Apply to the court for the cash seized to be forfeited to the Crown (section 79).

(b) **Statutory safeguards to the above powers of civil forfeiture include** -

(i) requirements that the officer must be lawfully on the premises and must have reasonable grounds for suspecting that there is cash on the premises before a search under section 72 can be done; (see section 72(1)); and

(ii) The officer must act in accordance with a search warrant or the approval of a senior officer if action is taken in the absence of a warrant (section 73(1)).

(iii) Additionally POCA mandates the Minister to establish a code of practice in connection with the exercise of powers conferred under section 72. (See section 74)

(c) The enforcing authority under this section of the Act (i.e. the ARA or the DPP) can apply to the Supreme Court to recover in civil proceedings property claimed to be obtained through unlawful conduct; (i.e. recovery order); (section 57) (ss. 57 – 71)

For these purposes, property includes cash (including postal orders; bankers' drafts, cheques of any kind, monetary instruments of any kind designated by the Minister), real property believed to be obtained directly or indirectly by or in return for or in

connection with unlawful conduct (i.e. conduct that is unlawful under the criminal law of Jamaica).

(d) A court can make an order for provision out of recoverable property (i.e. property subject to a recovery order). In deciding whether it is just and equitable to make such a provision the court must take into account–

(i) The degree of detriment that would be suffered if the order was made; and

(ii) The enforcing authority's interest in receiving the realized proceeds of the recoverable property;

(iii)Whether all four of these conditions are met:

- whether the respondent obtained the property in good faith;
- whether steps were taken after obtaining the property that would not have been taken if the respondent had not obtained the property; or whether steps were taken before the property was obtained which steps would not have been taken if the respondent did not believe that he would obtain the property;
- when the steps at (ii) were taken the respondent had no idea the property was recoverable; and
- if a recovery order is made, then by virtue of the steps taken by the respondent at (ii) the order would be detrimental to the respondent. (Section. 58(3), (4), (5)).

Amendments effected to the POCA since its passage in 2007

23. Since its passage in 2007 POCA has been amended to extend the list of predicate offences and offences in respect of which an assumption of criminal lifestyle can be made, to include offences under the Child Pornography (Prevention) Act; specified offences under the Sexual Offences Act; and related inchoate offences of aiding and abetting; incitement etc.. Offences under the Law Reform (Fraudulent Transactions) (Special Provisions) Act (The "LRFATSPA") which targets offences such as lotto scam activities will also be accorded similar treatment.

(a) In October 2013 further amendments were passed in Parliament to the POCA to, among other things, -

(i) Clarify the suspicious transactions reporting requirements **(section 94(4));**

(ii) Outline the powers that competent authorities designated under the POCA have in relation to their role of monitoring compliance with the AML requirements under the POCA. Accordingly, competent authorities therefore, among other things, have the power to -

- ✓ Conduct examinations; request information and direct an entity to comply with the requirements of the Act or regulations. The competent authority has enforcement powers to ensure compliance with such directions; and

- ✓ share information with regulatory counterparts and law enforcement agencies, both locally and internationally.
  (Section 91A)(See also paragraph 24 below)

(iii) Extend the obligations placed on a financial institution to an entity that has corporate responsibility for the development and implementation of group wide AML/CFT prevention, policies and procedures for the group of companies of which the financial institution forms a part. (One eg. of such an entity would be a financial holding company as defined in the BSA); (**Paragraph 1 (1) of the Fourth Schedule to the POCA)** [17]

(iv) Introduce a cash transaction limit of JMD One Million beyond which it is illegal for transactions to be undertaken in cash unless such transactions are undertaken with permitted persons (such as banks). (Section 101A) (Refer also to paragraph 25 below)

(v) Refine the provisions applicable to law enforcement activity to, for eg. allow for the disposal of seized assets which are in danger of depreciating in value before the substantive case is determined in the courts with provision being made for the safe custody of the proceeds of disposal to be available at the conclusion of the case to the Party adjudged by the court to be the Party entitled to those proceeds.

[17] Section 16 of the POCA

(vi) Effect several amendments to POC (MLP) Regulations. (Refer to paragraph 29 below)

The Competent Authority

24. The pre-POCA position under the financial legislation, which existed before the BSA, was that the Supervisor of Banks (a designated Competent Authority) had legal access to all records of the banks, merchant banks and building societies. POCA synchronized the position under the AML laws with that under the financial legislation then and that status quo is maintained under the BSA. As such not only is the role of the Competent authority defined under the POCA, but that Act expressly speaks to the Competent Authority's legal authority to access information surrounding STRs and Threshold Transaction Reports ('TTRs') under the POCA (refer sections 97(2)(e), 100 and Regulation 3(4) POC (MLP) Regulations).

The amendments to the POCA in 2013 also strengthened the oversight powers of the Competent Authority. Accordingly, a new section (section 91A) has been inserted in the law which outlines the additional functions of the Competent Authority. These additional functions are:-

(a) Requiring the regulated business to comply with registration and reporting procedures (if any) developed by the Competent Authority and issued by written notice;

(b) Undertaking inspections or verification procedures (either directly or through a third Party);

(c) Issuing directions to take certain measures to either prevent, detect or reduce the risk of money laundering or terrorism financing;

(d) Examining and making copies of information or documents in the possession or control of the regulated business and relating to the operations of that business;

(e) Sharing information pertaining to examinations conducted by the Competent Authority with the Competent Authority's regulatory counterpart, a supervisory authority, or the designated authority either in Jamaica or in another jurisdiction. This ability to cooperate is–

(i) Restricted to information which is not subject to protection from disclosures (such as matters that are covered by legal professional privilege); and

(ii) Not meant to operate in contravention of the prohibitions regarding 'tipping off'.

Non-compliance with the directives/requirements of the Competent Authority is an offence and subsection (6) of section 91A provides for penalties, which may be both criminal (fine not exceeding JMD$250,000 on conviction in the RM Court and fine not exceeding JMD$1m on conviction in the Circuit Court) and administrative (such as the revocation of an operating licence).

Cash Transaction Limits (Section 101A POCA)

25. POCA now has a transaction limit in respect of transactions conducted in cash (i.e. notes and coins issued by BOJ or issued by the authority responsible for the issue of notes and coins in another jurisdiction[18]).

(a) Section 101A of POCA states that, a person shall not carry out a cash transaction in excess of JMD$1,000,000.00 or its equivalent (at the date of the relevant transaction) in any other currency, unless such transaction is undertaken with a permitted person. A 'permitted person' is defined as a bank licensed under the Banking Act; a licensed deposit taking institution regulated by Bank of Jamaica; a person licensed under the Bank of Jamaica Act to operate an exchange bureau; or any other person that may be designated by the Minister as a 'permitted person' by Ministerial Order.[19] A person or transaction can also be

[18] Section 101A(6) POCA
[19] Section 101A(6) of the Proceeds of Crime (Amendment) Act, 2013

exempted from the cash transaction limit by Ministerial Order, if the Minister is satisfied that it is in the 'public interest' to permit such an exemption.

Meaning of 'permitted person' and verification of exempt person

(i) The permitted person category includes commercial banks, merchant banks/licensees under the FIA, building societies, cambios and persons so designated by virtue of an order from the Minister of National Security.

(ii) A person can be exempt from the cash transaction prohibition by virtue of an order from the Minister of National Security.

(iii) The order by which a designation as 'permitted person' is done or by which exempt status is conferred, is subject to Affirmative Resolution.[20] If therefore a person conducting business with a licensed deposit taking institution, attempts to conduct a transaction in excess of the statutory limit on the basis of having received a designation as 'permitted person' or exemption status, the licensed deposit taking institution should ensure it has sight of and retain a copy of the gazetted copy of that order of exemption prior to proceeding.

(b) Permitted persons may carry out cash transactions in excess of the cash transaction limit with any person. It should be noted that the prohibition does not apply to a payment made to, or by, a permitted person (Section 101A(2)).

(c) Permitted persons should not refuse to carry out cash transactions solely on the basis of a cash transaction exceeding the cash transaction limit. In facilitating cash transactions, permitted persons remain obliged to be reasonably sure that they do not facilitate a financial crime or other breaches of the law. (An advisory to this effect was issued by the BOJ in May 2014 – refer to Appendix II)

[20] The Interpretation Act defines "regulations' as including, inter alia, orders and, further states that, unless otherwise indicated, regulations come into effect, on the date of publication in the gazette. (Refer to sections 3 and 31)

(i) Licensed deposit taking institutions and cambios therefore need to be alert for circumstances in which cash transactions are conducted by persons connected with each other which each meet or is below the statutory transaction limit, but which collectively exceed such limit, as these could amount to a single transaction being conducted in a manner designed to avoid the cash transaction limit prohibition.

'Connected' for this purpose could mean – persons connected with each other by virtue of having the same residential or business address, familial bonds, same contact details or contact persons, or persons connected with each other by virtue of the existence of common principals, common shareholders; common trustees; or connected through the use of funds derived from the same source.

(d) Once a cash payment is being made to a permitted person by a person other than a permitted person, or payment is being received by a permitted person from a person other than a permitted person, then the permitted person should ensure it employs the requisite checks (appropriate in the circumstances) to satisfy itself that its services are not being used to allow a non-permitted person to circumvent the prohibition at subsection (1) of section 101A.

(e) See Appendix I for the matters considered by the Ministry of National Security in reviewing an application for designation as a permitted person.

STATUTORY AML OBLIGATIONS UNDER THE POCA & POC (MLP) REGULATIONS

26. Statutory AML obligations under the POCA regime can be found in **Section V of the POCA** and in the POC (MLP) Regulations and require the following:-

(a) Filing required disclosures where this is applicable in the circumstances and manner prescribed and related record keeping obligations (ss94-96 and 100);

(b) Filing TTRs (s. 102 & reg.3(1)) (refer also to paragraph 29(a)(iii);

(c) Complying with the directions of the Designated Authority in relation to required disclosures and TTRs (reg. 3(6))

(d) Complying with a requirement or direction issued by the Competent Authority (section 91A(5));

(e) Making the required cross border currency report in the manner indicated by the designated authority (s.101)(2) (reporting threshold is USD10,000), and

(f) Complying with other AML/CFT operational and regulatory controls under the POC (MLP) Regulations, 2007. (Refer to Paragraph 29 below)

27. **Suspicious Transaction Reports (STRs) (Sections 94 - 96 & 100 POCA)**

(a) **Section 94** makes it an obligation for a person to make a required disclosure where the circumstances described therein exist or arise. The required disclosure is a disclosure to the nominated officer; or a disclosure to the designated authority in the form and manner prescribed by the POCA legislation[21]. (Section 94(3))

(b) The circumstances are as follows:-

(i) There is knowledge or belief that another person has engaged in a transaction that could constitute or be related to money laundering (Section 94(2)(a)); and

(ii) The information or matter on which the knowledge or belief is based or which gave reasonable grounds for such knowledge or belief, was obtained in the course of a business in the regulated sector (section 94(2)(b));

28. **With regards to the STR obligations financial institutions should note -**

[21] See Form 1 in the Schedule, POC (MLP) Regulations, 2007

(a) There is a minimum 30 day period for institutions to file a report with the designated authority (i.e. 15 days from the date on which the suspicion is formed, for the person who forms the suspicion to report to the nominated officer and 15 days within receiving the report for the nominated officer to file the report with the designated authority);

(b) For persons in the regulated sector as defined by the POCA (Fourth Schedule) (i.e. financial institutions, financial holding companies or designated non-financial institutions), the duty to make required disclosures in relation to suspicious transactions, arises in relation to transactions engaged in, in the course of business in the regulated sector (i.e. business as a financial institution, financial holding company or designated non-financial institution) which resulted in the reporting person's knowledge or belief that another person has engaged in a transaction that could constitute or be related to money laundering. For persons not included in the regulated sector, the duty to make required disclosures in relation to suspicious transactions or suspicious activities, is reflected in section 100 of the POCA. This duty to report arises in relation to information or other matter obtained or discovered in the course of the reporting person's trade, profession, business or employment, resulting in the knowledge or belief that another person has engaged in money laundering.

(c) For financial institutions and designated non-financial institutions, required disclosures are to be made using Form 1[22].

(d) For the purpose of determining whether a required disclosure is to be made, a business in the regulated sector must identify all-

(i) Complex, unusual or large business transactions carried out with the business; and

[22] POC(MLP) Regulations, regulation 17

(ii) Unusual patterns of transactions, whether completed or not, which appear to be inconsistent with the normal transactions carried out by that customer with the business, and

(iii) All business relationships and transactions with any customer resident or domiciled in a territory specified in a list of applicable territories published by notice in a Gazette by a supervisory authority. **(Section 94(4)(b))**

(e) A business in the regulated sector must make a record of all transactions and matters reflected at d) above and these records are to be retained for a period of not less than seven years; (**Section 94(4)(a))**

THE POC (MLP) REGULATIONS, 2007

29. The bulk of the AML operational and regulatory control requirements can be found in these Regulations.[23] The operational controls and requirements are discussed below and include the following:-

(a) **Threshold Transaction Reporting ('TTR')**

(i) **Regulation 3(1)** sets out the threshold reporting requirements for financial institutions to report all cash transactions involving the "prescribed amount", as per the limits which have been tiered in relation to financial institutions[24]. (See paragraph 29(a)(iii) below). Cash transaction reporting requirements are not applicable to cash transactions carried out by a Ministry, Department of Government, statutory body or authority; a company in which the Government or an agency of Government is in a position to influence the policy of the company; an Embassy, High Commission, consular office or organization to which the Diplomatic Immunities and Privileges Act apply or

[23] A number of amendments were also effected to these Regulations with the passage of the Proceeds of Crime Amendment Act in October 2013 and these can be found in the First Schedule to the Amendment Act.
[24] Regulation 3(8).

any organization in relation to which an order is made under Section 3(2) of the Technical Assistance (Immunities and Privileges) Act;

(ii) **Regulation 4(2)** allows the Minister to grant an exemption from the threshold reporting requirement to financial institutions which apply for such exemption, in relation to established customers (defined as customers with whom the institution has done business for at least 12 months). Such exemption would be considered where:

1. the transaction or series of transactions involve the deposit into or withdrawal of monies held by such an established customer from an account in a financial institution;
2. the customer carries on: -
   - ✓ a retail business, not including the sale of motor vehicles, vessels, farm machinery or aircraft; or
   - ✓ a business declared by the Minister by order to be an entertainment business or a hospitality business for the purposes of this Act;
3. the account through which the transactions are conducted is maintained for the purpose of such business; **and** critically,
4. the amount of money involved is not over and above an amount that is reasonably commensurate to the lawful activities of the customer.

(iii) The threshold reporting limits[25] for financial institutions is as follows:-

1. Financial institutions other than cambios - US$15,000 or more or the equivalent amount in any other currency;
2. Cambios or bureau de change – US$8,000 or more or the equivalent amount in any other currency;
3. Remittance companies - US$5,000 or more or the equivalent amount in any other currency.

[25] POC (MLP) Regulations, 2007 regulation 3 (7) & (8).

(iv) Financial institutions will be required to apply appropriate due diligence mechanisms to ensure that their transactions do not breach the cash transaction limits. Since the passage in 2013 of the amendments to the POCA which introduced the cash transaction limit of JMD 1 million, and based on the current exchange rate (JMD 117.44 to USD1 as at 17/08/2015)), it would be illegal for a person to conduct a cash transaction that amounts to, or exceeds USD10,000 (due to section 101A of the POCA) unless :-

1. Such a transaction is being conducted with a permitted person;

2. Such a transaction is being conducted with a person which has been designated a 'permitted person' by order of the Minister of National Security; or

3. The person or transaction has itself been exempted from the cash transaction prohibition by order of the Minister of National Security.

The cash transaction limit provisions under the POCA, will therefore require financial institutions to apply appropriate section 101A due diligence for transactions of USD10,000 and above to ensure that such transactions are not facilitated in contravention of the cash transaction limit. (Refer to paragraph 25 above)

(v) Under the TTR regime the Designated Authority can request information from financial institutions on any of the following persons exempted under the TTR regime – i.e. a Ministry, department or agency of Government; a statutory body or authority or a Government company. (Refer Regulation 3(3)). Additionally, the Designated Authority has the power under the regime to issue directions to a regulated business in relation to matters arising from TTRs and STRs filed. These directions can be issued in relation to: -

1. previous or current reports;

2. the provision of information regarding a report at 1.;
3. the provision of additional information in response to queries concerning specific matters arising from a report at 1. including:
   - ✓ due diligence procedures followed in relation to a specific transaction;
   - ✓ persons authorized to sign on a specific account;
   - ✓ errors identified in the report; and
   - ✓ such other matters specified in the directions. (Regulation 3(6))

(b) **KYC/ Customer Due Diligence ('CDD') requirements**

(i) **Risk Profile**

Financial institutions are required to establish a risk profile regarding all business relationships and one-off transactions to allow for determination as to which of these relationships is high risk. (Regulation 7A[26]) The basis on which such profiles are established should be guided by the respective risk assessments undertaken as discussed in these Guidance Notes at Section IV below. 'High risk' relationships or transactions are categorized in the law at paragraph 2 of regulation 7A and include the following –

1. Politically Exposed Persons ('PEPs');
2. Trustees;
3. A person who is not ordinarily resident in Jamaica;
4. A company having nominee shareholders, or shares held in bearer form, and
5. A member of such other class or category of persons as the supervisory authority may specify by notice published in the gazette.

(ii) **Reasonable Due Diligence**

[26] Proceeds of Crime (Amendment) Act, 2013, First Schedule

Financial institutions are mandated by regulation 7A(3) to carry out reasonable due diligence in the conduct of every transaction to ensure the transaction is consistent with an institution's knowledge of the transacting Party's -

1. business, trade or profession,
2. risk profile, and
3. stated source of funds involved in the transaction.

In addition to the foregoing financial institutions are also mandated in this regulation in relation to each transaction conducted, to verify the identity of the transacting Party as well as the source of funds involved in the transaction.

Regulation 7(5) contains the following definition of "customer information", "*Customer information includes applicant for business's full name, current address, taxpayer registration number or other reference number, date and place of birth (in the case of a natural person) and, where applicable, the information referred to in regulation 13(1) (c)*"; (**See also section 122(1) POCA**) **which outlines the KYC information a financial institution must be in a position to provide pursuant to customer information orders**.

(iii) In addition to the foregoing, the POC (MLP) Regulations, 2007 require the following -

1. Periodic updates of customer information must be carried out at least once every seven years or at more frequent intervals as warranted by the risk profile of the business relationship; This is applicable to existing and new customers. (Regulation 7(1)(c) & (d),19[27]);

[27] Existing customers transactions dating back to March 2007.

2. Transaction verification procedures[28] must be applied particularly in the circumstances specified in regulation 7(3) which include cases where - the transaction meets the TTR; transactions appear to be linked; wire transfer transactions are being conducted; a required disclosure (STR) is to be made; or there is doubt about the accuracy of any previously obtained evidence of identity;

3. KYC details must be retained for electronic funds transfers, and in respect of transfers which exceed USD1,000 or the equivalent amount in any other currency, the KYC details must include -

   - ✓ a national identification number;
   - ✓ the customer identification number; or
   - ✓ the date and place of birth of the person who places the order for the transfer and the holder of the account that is the source from which the funds are transferred. (Regulation 9(2A)[29])
   - ✓ The law reflects that the business from which the transfer originates must provide the KYC details to the business to which the funds are transferred within three days of being requested so to do by the business to which the funds are transferred. (Regulation 9 (2B))

4. Procedures must be in place to ensure that the identities of both principals and agents are obtained in the case of transactions being conducted by a person on behalf of another; (Regulations 11, 12 and 13)[30];

[28] Taking such measures specified in the procedures of a regulated business that will produce satisfactory evidence as to the purpose of and intended nature of the business relationship or one-off transaction – (POC (MLP) Regulations, 2007 - regulation 7(2)(a))
[29] FATF Recommendation 16 (Wire Transfers) and the related Interpretive Note.
[30] POC (MLP) Regulations, 2007

5. Procedures must be in place to ensure that the identities of the beneficiaries and ultimate beneficial owner of the property or funds which are the subject of the transaction and/or business relationship, are obtained; (Regulation. 11, and 13[31]);

6. Financial institutions must ensure the retention of records not only for identification records, but also for transaction records; (Regulation 14)

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

8. Financial institutions must ensure that the CDD update requirements are applied to existing customers. (Regulation 19) It should also be noted regulation 19 also reflects that financial institutions are not required to obtain information or evidence in respect of any transaction conducted prior to the relevant date (which is March 29, 2007). Financial institutions will however need to ensure that in balancing the requirements of regulation 19, they retain the ability to deal effectively and appropriately with issues that may arise in respect of records or transactions which pre-date the relevant date of March 29, 2007.

   ✓ Financial institutions must ensure that required disclosures are filed on the statutory STR Form 1 (See Form I in the Schedule to these Regulations)

9. Financial Institutions other than remittance services, can apply a de minimis transaction amount of US$250.00 below which the regulation 7 (identification procedures) will not be required unless the nature of the transaction is suspicious (see also Section V – paragraph 152 on de minimis transactions);

[31] POC (MLP) Regulations, regulation 11 and 13 – First Schedule to the POC (Amendment) Act, 2013;

30. Financial institutions should note that the above AML obligations comprise specific requirements that FATF requires jurisdictions to have in place in order to be considered as having effective KYC/CDD regimes. In complying with obligations under POCA and its Regulations financial institutions should consult with their respective legal advisors.

Terrorism Prevention Act, 2005 ("TPA")

31. The TPA was passed in 2005, and amended in 2010, 2011 and 2013. The Act outlines the following as 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;

Entering into or facilitating, directly or indirectly, any transaction in respect of property owned or controlled by or on behalf of a terrorist group;

Providing any financial or other related services in respect of that property for the benefit of or at the direction of a terrorist group;

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)**

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.

32. 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 property[32]-

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

(iv) Property 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

[32] TPA Sections 2(2)-(7)

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.

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.

33. The TPA also 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; **(section 14)**

(b) report all suspicious transactions to the Designated Authority[33], which under the TPA is, the CTD of FID. or such other person as the Minister may substitute by order, subject to Affirmative Resolution and published in the Gazette; **(section 15[34])**

(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; **(section 18)**

(d) establish and implement programmes, policies, procedures and controls for enabling them to fulfil their duties under the TPA. Towards this end, financial institutions must designate a Compliance Officer at management level and arrange for independent audits to ensure that their compliance programmes are effectively implemented. **(section 18)**

34. Breaches of the obligations reflected in paragraph 33 are offences that will attract the following penalties:-

(a) Under Sections 15 and 16 an individual is liable on conviction, to a fine not exceeding JMD$1 million dollars, and in the case of a body corporate, to a fine not exceeding JMD$3 million dollars.

(b) Unauthorised disclosures by persons of information relating to 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, unless such disclosure is made to an attorney-at-law for the purpose of obtaining legal advice, facilitating the investigation, or any proceedings which might be conducted following the investigation, conviction, to imprisonment for a term not exceeding two years and/or a fine of not more than JMD$2 million or both in the case of an individual and in the case of a body corporate, to a fine not exceeding JMD$6million dollars. (Section 17)

[33] In March 2006 the Minister designated the CTD of the FID the Designated Authority for the purposes of reporting obligations and other specific obligations outlined at sections 15-18 of the TPA. Section 15 TPA has been amended to indicate that the CTD of the FID is the Designated Authority.
[34] The Terrorism Prevention (Amendment) Act, 2013, new section 15(1) and new subsection (9).

(c) For breaches of sections 15(7) and 17(2), tipping off offences –

(i) Disclosing the existence of a report under section 15(3) to any person other than the designated authority (refer to section 15(6)), the penalty on conviction in an RM court in the case of an individual is a fine not exceeding JMD 1million and/or imprisonment for a term not exceeding 12 months; and in the case of a body corporate, the penalty on conviction is a fine not exceeding JMD 3 million.

(ii) Knowing or suspecting that a report has been made to the designated authority and disclosing any information or matter relating to a report under section 15(3) or 16(3) (refer to section 17(2)), the penalty on conviction in an RM court in the case of an individual is a fine not exceeding JMD 2million and/or imprisonment for a term not exceeding 2 years; and in the case of a body corporate, the penalty on conviction is a fine not exceeding JMD 6 million.

35. The following Table outlines the enforcement powers under the TPA.

AREAS OF ENFORCEMENT UNDER THE TPA

Areas of Enforcement	**Section of Act/Regs.**	**Responsible Authority**	**Additional Information**
Listed entity procedures	Sec. 14	DPP	
Duty of entities to report	Sec. 15	CTD of the FID (as of Mar. 2006) DPP (in 2005)	The Act now reflects the designated authority is the CTD of the FID.
Duty to file complex or	Sec.16(3)	CTD of the FID	"

unusual large transactions		(as of Mar. 2006) DPP (in 2005)	
Duty to file STRs	Sec. 16(3A)	CTD of the FID (as of Mar. 2006) DPP (in 2005)	"
Tipping off	Sec. 15(3) Sec. 16(3) Sec. 17(2)	CTD of the FID (as of Mar. 2006) DPP (in 2005)	The Act now reflects the designated authority is the CTD of the FID.
Implementation of regulatory controls to prevent TF	Sec.18	Competent Authority[35] BOJ (as of May 2015) FSC (as of May 2015) Minister of Finance or other person designated as Competent Authority. (2005)	
Areas of Enforcement (cont'd…)	**Section of Act/Regs.**	**Responsible Authority**	**Additional Information**
Monitoring Orders	Sec. 19 Sec. 20	Relevant Authority DPP (2005)	i.e. either the DPP or the CTD of the FID.
Examination and production orders	Sec. 21	Relevant Authority DPP (2005)	i.e. either the DPP or the CTD of the FID.
Search Warrant	Sec. 23	Physical execution is	

[35] Prior to 2015 this function in practice – was undertaken by the BOJ for DTIs, FHCs, credit unions, cambios and remittance services and by the FSC for persons licensed or registered under the Insurance Act, the Securities Act and the Pensions Act.

		achieved by the Constable named in the warrant.	
Forfeiture orders ss.28-32	Secs. 28-32	Relevant Authority DPP (2005)	i.e. either the DPP or the CTD of the FID.
Restraint orders	Secs. 34-43	Relevant Authority DPP (2005)	i.e. either the DPP or the CTD of the FID.
Disposal (i.e. resolution of) property seized, restrained etc.	Sec. 44	Relevant Authority DPP (2005)	i.e. either the DPP or the CTD of the FID.

36. Sections 19-44 of TPA treat with enforcement and investigatory tools such as Forfeiture Orders (section 28), Pecuniary Penalty Orders (section 28(5A)), Restraint Orders (sections 34-41), Search and Seizure Warrants (sections 23-27), and Account Monitoring Orders (sections 19 and 20).

The foregoing orders operate with similar effect to those described under the POCA subject to the following differences:-

(a) <u>Account Monitoring Orders</u>

These remain in effect for 3 months. The applicable sections do not reflect that the duration of the order can be extended.

Account information is not defined, but, as is the case with the POCA, the monitoring order is applicable to information regarding transactions conducted through an account by a particular person with the institution. Reference to transactions conducted through an account includes the making of a fixed term deposit including the transfer of funds deposited or any part thereof at the end of the term, a financial investment, and the opening, existence or use of a deposit box held by the institution.

There is no express wording that reflects the order takes effect regardless of any restriction on the disclosure of the information however imposed, as is the case under the POCA at section 126(7).

(b) <u>Examination and Production Orders (sections 21 and 22)</u>

The DPP or the CTD of the FID can also either apply to the court for information or documents to be made available for examination or for a production order. The application is made ex parte in writing, and if granted, the subject entity would be directed by the judge to make the information or documents available for examination by a constable named in the order, or to produce the information or document to the constable. An order to produce does not require the constable to remove or retain any accounting records (including ledgers, daybooks, cash books and account books) used in the ordinary business of banking). An order can provide for these documents to be examined or copied wherever they are located.

(c) Statutory safeguards to the powers of forfeiture

Statutory safeguards to the above powers similar to those discussed above in relation to the POCA are also included in the TPA as follows:

(i) In considering whether a forfeiture order should be made the Court must take into account –

1. Third Party rights and interests in the property;
2. The gravity of the offence concerned;
3. Any hardship that might reasonably be expected to be caused by the order;
4. The use that is ordinarily made of the property or the intended use of the property; (section 28(5))

(ii) Not less than 14 days written notice of an application for a forfeiture or pecuniary penalty order must be given by the enforcing authority (i.e. DPP or CTD of the FID) to the Defendant and any other person it is believed to have an interest in the property targeted for forfeiture. Additionally, a copy of the notice must be published in a daily newspaper printed and circulated in Jamaica; (section 28(2)).

(iii) Persons claiming an interest in the property targeted for forfeiture may apply to the court for an order and the Court, if it is so satisfied shall make an order declaring the nature, extent and value of the person's interest in the property. Before such an order is made the court must first be satisfied that the applicant was not in any way involved in the commission of the offence; that the person

acquired his interest for sufficient consideration and without knowing or having reasonable grounds to suspect that at the time the property was acquired, it was used in, or derived from, obtained or realized directly or indirectly from, the commission of a terrorist offence; (section 31(2)).

Terrorism Prevention (Reporting Entities) Regulations, 2010

37. Section 47 of the TPA allows for Regulations to be made for giving effect to the provisions of this Act. Regulations under the TPA are subject to Affirmative Resolution. The Terrorism Prevention (Reporting Entities) Regulations were promulgated in March 2010. Under these Regulations, reporting entities include the financial institutions to which these Guidance Notes apply. These Regulations outline the operational procedures that must be maintained by financial institutions particularly when contemplating the commencement of a business relationship or conducting a one-off transaction. These regulations therefore largely mirror the POC (MLP) Regulations and require financial institutions to establish and maintain appropriate procedures in relation to establishing a risk profile for all business relationships and one-off transactions, identification of customers (including identification of the agent, ultimate beneficial owner or person who ultimately controls a legal person), record-keeping (minimum 7 year retention period), internal controls, communication, and training of employees. These Regulations also prescribe the requisite Declaration Forms for transactions which the reporting entity knows or suspects may constitute a terrorism offence; and for the quarterly reports as to whether or not the reporting entity is holding property etc. in respect of a listed entity.

38. Under the CFT framework, an institution is required to report whether:-

(a) The institution is, or is not, in possession of property for a listed entity (section15); or

(b) The institution is, or is not, in possession of property for a person included on the UN consolidated listing of individuals and entities pertaining to Al-Qaida pursuant to United Nations Counter-Terrorism Security Council Resolution 1267 (1999) – Afghanistan (section 15); or

(c) The institution is of the view that a transaction conducted or being conducted or about to be conducted constitutes a transaction of the kind described at section 16 of the TPA (ie. suspicious[36], unusual, complex[37] etc.),

The requisite report must be made to the designated authority[38] using either Form 1 (re: a report in relation to a) or b), or Form 2 (re: a report in relation to c)) provided in the Schedule to the Regulations.

Financial Investigations Division Act, 2010

39. The Financial Investigations Division Act ("FIDA") codified the establishment of the Financial Investigations Division ("FID") which has been in operation since 2002, and is a Department of the MOFP. The FIDA also provides the statutory basis for the operations and objectives of the FID and outlines these as being to: -

(a) Investigate all categories of financial crime;

(b) Collect information and maintain intelligence databases on financial crime;

(c) Maintain an arm's length relationship with law enforcement agencies and other authorities of Jamaica and foreign States, and with regional and international associations or organizations, with which it is required to share information;

(d) Exercise its functions (section 5) with due regard for the rights of citizens. These functions include collecting, requesting, receiving, processing, analyzing and interpreting information relating to financial crimes; and transaction reports and any other reports made to or received by the Division; promoting public awareness and understanding of financial crimes and the importance of their elimination from the society; formulating and implementing guidelines and policies and an annual plan39 for the control and prevention of financial crimes; and the compilation and publication of statistics on reports made to the Division, the investigations carried out by the Division, and the prosecution of financial crimes and conviction of persons for financial crimes. The Division may also provide information on typologies and other

[36] The Terrorism Prevention (Amendment) Act, 2011 section 16(3A)
[37] The Terrorism Prevention (Amendment) Act, 2011 section 16(3)
[38] The Terrorism Prevention (Amendment) Act, 2013, new section 15(1)
[39] As approved by the Minister of Finance.

materials relating to financial crimes to public bodies, and, after consultation with the Competent Authority, give guidance to financial institutions and designated non-financial institutions regarding their obligations under the FIDA and any other enactment. (Sections 3 & 4)

40. The FID is the designated authority to receive reports under the POCA (section 91(1)(h); the TP (Amendment) Act (section 15)); and The UNSEC Implementation Act (section 5(1)). FID statistics and publications including advisories to financial institutions and to designated non-financial institutions can be accessed from its website at www.fid.gov.jm.

41. On June 05, 2014 the FID was accorded membership with the Egmont Group of Financial Intelligence Units[40].

Criminal Justice (Suppression of Criminal Organizations) Act, 2014

42. This Act criminalizes forming or establishing, participating in or being part of, a criminal organization, or knowingly facilitating the commission of a serious offence by or on behalf of a criminal organization.

Dangerous Drugs Act, 1948 (amended 2015)

43. This Act makes it a criminal offence for any person to import, export, cultivate, manufacture, use, sell, transport or otherwise deal in opium, ganja, cocaine, morphine, or any derivatives thereof. In March 2015 this Act was amended to, among other things, modify the penalties applicable for the possession of specified small quantities of ganja and the smoking of ganja in specified circumstances, and for a scheme of licenses, permits and other authorizations for the cultivation or acquisition or use of ganja for

[40] Co-Chairs **St**atement 22nd Plenary Of The Egmont Group of Financial Intelligence Uni**ts,** 01-6 June 2014 www.egmontgroup.org

medical, therapeutic or scientific purposes. This amendment became effective on 15 April 2015. In this regard the following should be noted:-

(a) The possession of ganja not exceeding 2 ounces amounts to a contravention of the Act and is a punishable matter which will result in –

(i) notice that a contravention has occurred and giving the offender 30 days (or such longer period as may be specified in the notice) to pay a fixed penalty of $500;

(ii) failure without reasonable cause or excuse to pay the penalty within the time period specified, is an offence for which the penalty on conviction in a Petty Sessions Court is to perform unpaid community service for between not less than 40 nor more than 360 hours; or a fine of $2,000.
(section 7(F) &(G))

(b) The Cannabis Licensing Authority is established by section 9A for the purpose of enabling the establishment of a lawful regulated industry in hemp and ganja for medical, therapeutic or scientific purposes. This Authority has the power to make regulations (with the approval of the Minister of Justice) for the issue of licenses, permits and authorizations for hemp and ganja for medical, therapeutic or scientific purposes. The Authority is also charged with ensuring that regulations made by the Authority do not contravene Jamaica's international obligations.

(c) The possession of over 2 ounces of ganja remains a criminal offence, unless that possession is for religious purposes in adherence with the rastafarian faith; or for medical or therapeutic purposes as prescribed or recommended in writing by a registered medical practitioner or other health practitioner or class of practitioners approved for that purpose by the Minister of Health by gazetted order; or for the purposes of scientific research by a duly accredited tertiary institution or otherwise approved by the Scientific Research Council or such other body prescribed by the Minister of Science, Technology, Energy & Mining (section 7C).

Firearms Act, 1967

44. This Act deals with the regulation and licensing of the sale, purchase, acquisition, ownership and other dealings with regard to firearms. The Act was last amended in 2010.

Law Reform (Fraudulent Transactions) (Special Provisions) Act, 2013

45. This Act, criminalizes, among other things,
(a) obtaining property by false pretence (section 3);
(b) inviting persons to Jamaica by a false pretence (section 4);
(c) using premises for purposes which constitute an offence under this Act (section 5);
(d) using an access device[41] or other means to transfer or transport money or monetary instrument either within Jamaica, or between Jamaica and a place outside of Jamaica;
(e) making, repairing, buying, selling exporting or importing, without lawful justification or excuse any instrument, device, apparatus, material or thing that a person knows has been used or is intended for use for copying data from an access device or forging or falsifying an access device; whilst knowing or having reasonable grounds to believe, that the money or monetary instrument involved in such transfer or transportation constitutes or is substantially related to the proceeds of some form of unlawful activity (section 6);
(f) stealing, forging or falsifying an access device; knowingly using an access device that has revoked or cancelled with an intent to commit an offence; or knowingly possessing or using or trafficking in an access device or a forged or falsified access device that has been obtained made or altered by an act or omission constituting an offence under this Act, any other law or by an act or omission constituting an offence

[41] "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, and any other means of access that can be used alone or with another device, to obtain a benefit or other thing of value, or that can be used to initiate a transfer of money;" – section 2 – The Law Reform (Fraudulent Transactions)(Special Provisions) Act, 2013.

in a country other than Jamaica but which act or omission would constitute an offence had it been committed in Jamaica (section 8).

(g) knowingly obtaining or possessing, transmitting, distributing etc, identity information including any biological information, name, address, date of birth, written signature, e-mail address, digital signature, user name, credit or debit card number, financial institution account number, Taxpayer Registration Number ('TRN'), Social Security Number, or any other unique personal identification number or password (section 10).

Cyber Crimes Act, 2015

46. This Act came into effect in December 2015 and repealed and replaced the earlier Act of the same name. It allows for the imposition of criminal sanctions for cybercrimes, and criminalizes, among other things:-

(a) Unauthorised access to computer program or data (section 3);

(b) Access to any program or data held in a computer with intent to commit or facilitate commission of an offence (section 4);

(c) Doing any act which it is known is likely to cause an unauthorized modification to the computer whether or not the act is directed at a particular program or data, or directed at a particular program or data held in a particular computer and whether or not the modification is temporary or permanent (section 5);

(d) The unauthorised access to any computer to access a service directly or indirectly or the unauthorised interception (directly or indirectly) of a function of any computer. Interception in this case includes listening, viewing or recording a function of the computer or the substance of such function (and excludes interceptions permitted under the Interception of Communications Act) (section 6);

(e) The unauthorized, or wilful failure, interruption or obstruction, of the operation of a computer, or the denial of access to, or impairment of, any computer program or data stored in the computer (section 7);

(f) Fraudulently altering or interfering with data or a computer program with the intent of gaining an advantage for oneself or for another (section 8);

(g) using a computer to send to another person any data that is obscene, constitutes a threat, or is menacing in nature; with the intention of causing or being reckless as to whether the sending of the data causes, annoyance, inconvenience, distress, or anxiety, to that person or any other person (section 9);

(h) Possessing, receiving, manufacturing, selling, importing, distributing, disclosing or otherwise making available, a computer, access code or password or any other device adapted primarily for the purpose of committing an offence at sections 3-9 (section 10);

47. The law states that where any of the foregoing offences involves a 'protected computer', an offender is liable on conviction before the Circuit Court to a fine or imprisonment for a term not exceeding 25 years, or both such fine or imprisonment, which is a higher penalty than included in the specific sections. A 'protected computer' is one which the offender knows or ought reasonably to know, is a computer which is involved with or used in connection with security, defence or international relations for Jamaica; the existence of a confidential source of information relating to the enforcement of the criminal law of Jamaica; the provision of services directly communications infrastructure, banking and financial services, public utilities, public transportation etc. (section 11);

48. Inciting, attempting, aiding or abetting the commission of any offence under sections 3-10 is also an offence and the person shall be liable to the same penalty as the substantive offence under this Act (section 12).

Other Offences Relating to Fraud, Dishonesty, and Corruption

49. There are several statutes relating to these offences. Some examples are certain offences under the Companies Act, the Income Tax Act, the Customs Act, the Stamp Duty Act, the Charities Act, the Larceny Act, the Corruption Prevention Act, the Copyright Act and other enactments relating to the conferment of or protection and administration of

intellectual property rights, and under the BSA and the BOJA, the Credit Reporting Act, the Securities Act, the Insurance Act, and the Perjury Act.

THE PREVENTION OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

50. Recommendation 7 (on targeted financial sanctions relates to the prevention of the proliferation of weapons of mass destruction) of the revised FATF Forty Recommendations, 2012 requires countries to implement targeted financial sanctions relating to the prevention of weapons of mass destruction proliferation which are contained in the relevant UN Security Council Resolutions that have thus far been issued in relation to the Democratic People's Republic of Korea (DPRK) (Resolution 1718 (2006)) and successor resolutions thereto, and in relation to Iran (Resolution 1737(2006)) and successor resolutions thereto[42].

(a) Targeted financial sanctions include – freezing and prohibiting dealings in funds or other assets of designated persons and entities; and activity based financial prohibitions such as preventing the provision of financial services, financial resources or financial assistance related to the supply, sale, transfer, manufacture, maintenance, or use of items, materials, equipment, goods and technology prohibited by the UN Resolutions[43].

(b) Compliance with these mandates to apply targeted financial sanctions requires the ability to be in a position to identify any related suspicious activity and to propose

[42] Refer also to FATF Guidance on the Implementation of UNSEC Resolutions to Counter the Proliferation of Weapons of Mass Destruction, June 2013. See also the UN Charter – "*The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations.*" (Article 41 – Cap VII) "*The Members of the United Nations agree to accept and carry out the decisions of the Security Council in accordance with the present Charter".* (Article 25 – Cap V)

[43] Refer also to FATF Guidance on the Implementation of UNSEC Resolutions to Counter the Proliferation of Weapons of Mass Destruction, June 2013 (paragraph 15 page 7; and Annex C)

additional persons and entities to the UN Committees for designation. Accordingly, UN Member States have an obligation to ensure the necessary supporting framework is in place to allow for the:-

(i) Designation mechanisms to allow for the nomination of persons to the UN Committees for designation;

(ii) Implementation of the required measures and controls that will allow for the following measures to be applied -

1. Identification of transactions, services or other relationships that would be prohibited by the UN SEC Resolutions;

2. Appropriate reporting of the prohibited transactions, services or other relationships that have been identified; and

3. Effective application of the required targeted financial sanctions in the manner required by the UN SEC Resolutions;

(iii) Appropriate cooperation across borders and within borders (i.e. between countries and among national authorities;

(iv) Protection of the rights of innocent third parties (eg. de-listing mechanisms and unfreezing of assets); and

(v) Orderly application of sanctions - that is, the application of sanctions through mechanisms that adequately address corresponding risks (if any) to financial and payment systems posed by the application of sanctions and which address the protection of the rights of innocent counter-parties acting in good faith. This could include for example, mechanisms designed to-

1. prevent asset flight;

2. facilitate authorization of certain payments by designated banks;

3. permit payments due under prior contracts entered into prior to a person or entity being listed or designated provided such contracts do not involve services, items or assistance prohibited by the Resolutions and provided

payments are not being made directly or indirectly to a designated person or entity;)[44].

United Nations Security Council Resolution Implementation Act

51. The United Nations Security Council Resolution Implementation Act was passed in November 2013 and is designed to achieve Jamaica's 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.

52. This Act is an enabling legislation which forms the basis for Jamaica to respond to directives or resolutions issued by the UN SEC by promulgation of the requisite Regulations under this Act. Accordingly, the Act defines certain terminology (section 2)–

(a) "asset" (property of any kind, tangible or intangible, moveable or immoveable, however acquired whether wholly or jointly owned directly or indirectly by a person or entity that is proscribed under section 3(2)(a) or a person or entity acting on behalf of such a proscribed person or entity);

(b) "designated non-financial institution" (i.e. a person designated under the POCA as well as persons listed at section 15 of the TPA);

(c) "financial institution" (same as FIDA similar to POCA and TPA)[45];

(d) "relevant authority" (that is, regulator of financial institutions or financial services – such as the BOJ and the FSC), regulator of designated non-financial institutions (such as the General Legal Council, the Real Estate Board, the Betting Gaming and Lotteries Commission and the Casino Commission); border control authorities (such as Jamaica Customs Agency and PICA[46]), defence authorities (such as the Coast

[44] Refer also to FATF Guidance on the Implementation of UNSEC Resolutions to Counter the Proliferation of Weapons of Mass Destruction, June 2013 (Annex A)

[45] FIDA is the only other statute which refers to cooperative societies which undertake credit union business neither the POCA nor the TPA reflect this qualification in the reference to cooperative societies in the respective definitions of 'financial institution'.

[46] Passport, Immigration and Citizenship Agency

Guard and the JDF), entity with responsibility for foreign relations (i.e. MFAFT[47]), the Jamaica Constabulary Force; any other entity to whom a UN sanction enforcement law requires information or a document to be given;

53. The Act provides for the following:-

(a) 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 prescribed by regulations made under regulation 3 and to report whether they are, or are not, in possession of property for a person who is so prescribed (section 5). These reports are to be made to the designated authority, which is defined in the Act, to be the CTD of the FID under the FIDA, (section 5(1)). Reporting in this regard must be done in compliance with any directions that may be given by the designated authority, (section 5(4)); and the fact that a report has been made must not be disclosed to any other person, (section 5(6)). These reports are due once every four calendar months. Reports are also due upon request of the designated authority. (section 5(3))

(b) Provides statutory protections for persons with reporting obligations under this Act, from civil or criminal liability for breaches of confidentiality; (sections 5(5) re: reporting to the designated authority and 18 re: disclosures to the relevant authority)

(c) Provides for the designation of any provision of a law in Jamaica as a UN sanction enforcement law. This designation is done under section 9 and can only be done to the extent that it gives effect to a decision made by the UNSEC under Chapter VII of the UN Charter and which Jamaica would be obliged to carry out under Article 25 of the UN Charter.

(d) Provides for monitoring compliance with any UN sanction enforcement law by empowering the regulated authority by written notice to request from any person the information or documents specified in the notice. Non-compliance with this request constitutes an offence (sections 14 and 15) however a person is not required to give any

[47] Ministry of Foreign Affairs and Foreign Trade

information or document in response to a request, if to do so would violate legal professional privilege (section 14(7));

(e) Provides for the development of regulations to give effect to the Act (such as programmes and policies to be implemented by entities to ensure compliance with the Act; forms of reports or returns to be made under the Act, prescription of penalties)(section 21) and to give effect to the UNSEC Resolutions (section 3)

(i) When a directive or resolution is issued from the UN SEC mandating members to take certain actions and/or refrain from activities pursuant to such directive or mandate, Jamaica would then issue the requisite Regulation under this Act giving effect to such a decision and outlining the specific parameters of compliance (section 3). One set of Regulations in this regard was issued simultaneously with the passage of this Act in relation to the jurisdiction of the Democratic People's Republic of Korea.

54. The UNSEC Resolutions Implementation (Asset Freeze - Democratic People's Republic of Korea) Regulations, 2013[48] 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, (paragraph 50 above).

55. These Regulations criminalize the following activities:-

(a) The holding of, using or dealing with freezable assets, that is, assets owned or controlled by a designated entity. A designated entity is defined as an entity designated in Annex I or Annex II to UNSEC Resolution 2087 (2013); an entity designated by the UN Sanctions Committee or by the UNSEC for the purposes of paragraph 5(a) of UN Resolution 2087(2013) as a person in respect of which countries must freeze immediately funds, or other financial assets and economic resources which are - in their territories, owned or

[48] Schedule to The UN SEC Resolutions Implementation Act, 2013

controlled directly or indirectly by such designated entity, an entity acting on behalf of, or at the direction of an entity that has been designated, or an entity owned or controlled by such designated entity;

(b) Allowing freezable assets to be used or dealt with;

(c) Facilitating the use of or dealing with, freezable assets;

(d) Directly or indirectly making a freezable asset available to a designated entity otherwise than pursuant to a written notice allowing this to be done pursuant to regulation 7. (regulations 5(1) and 6(1))

56. The Regulations stipulate the penalties that are applicable on conviction for an offence; (regulation 5(2), regulation 6(2)) and establishes a mechanism by which the owner or holder of a freezable asset may obtain authorization to use or deal with a freezable asset in a specified way, or for a freezable asset to be made available by the owner or holder thereof, to a designated entity (regulation 7).

Areas of Enforcement Under UNSEC Implementation Act, 2013 And UNSEC Implementation (Asset Freeze-DPRK) Regulations, 2013

Areas of Enforcement	**Section of Act/Regs.**	**Responsible Authority**	**Additional Comments**
Duty of entities to report	Sec. 5	CTD of the FID	It is a defence that a person charged has a reasonable excuse for not making the report. 'Reasonable excuse' is not defined.
Tipping off	Sec. 5(6)	CTD of the FID	
Injunction to prevent breach of an Implementing Regulation	Sec. 7	Attorney General	
Areas of Enforcement (cont'd…)	**Section of Act/Regs.**	**Responsible Authority**	**Additional Comments**
Monitoring compliance	Sec. 13	Relevant Authority	See paragraph 52 above for definition of 'relevant

			authority'.
Implementation of regulatory controls to ensure compliance	Sec. 21 & Regs. under the Act	Minister of Foreign Affairs and Foreign Trade for issuing Regs. under the Act.	No Regulations developed yet. See also paragraph 52 above for guidance on regulatory controls.
Reporting form	Sec. 21 & Regs. under the Act	Minister of Foreign Affairs and Foreign Trade for issuing Regulations under the Act.	No Regulations developed yet.
Offences under the Act			
Failing to make a determination on a continuing basis whether there is possession or control of assets owned or controlled by or on behalf of a designated entity. (Sec. 5(2))	Sec. 5(7)	CTD of the FID	
Failing to report whether or not there is possession or control of assets owned or controlled by or on behalf of a designated entity. (Sec. 5(3))	Sec. 5(7)	CTD of the FID	
Failing to comply with a direction of the designated authority in making a report under section 5(3). (Sec. 5(4))	Sec. 5(7)	CTD of the FID	
Tipping off in relation to a report made under section 5(3). (Sec. 5(6))	Sec. 5(7)	CTD of the FID	
Areas of Enforcement (cont'd…)	**Section of Act/Regs.**	**Responsible Authority**	**Additional Comments**
Contravention of a UN sanction enforcement law.	Secs. 10 & 11	Relevant Authority (defined in para. 52)	An offence is not committed by a body corporate if it

			proves that it took reasonable precautions, and exercised due diligence to avoid the contravention concerned. (S. 11(3)) Compliance is monitored by the Relevant Authority under s.13 of the Act.
Attempting, conspiring, inciting, aiding, abetting, counselling or procuring the commission of any offence under sec. 10 or 11.	Secs. 10(3) & 11(4)	Relevant Authority	Compliance is monitored by the Relevant Authority under s.13 of the Act.
Listed entity procedures	Reg. 3	CTD of the FID Relevant Authority	Reports are done to the CTD of the FID under s.5 of the Act. Compliance is monitored by the Relevant Authority under s.13 of the Act.
Permission to use or deal with a freezable asset.	Reg. 7	MFAFT by written notice.	Applications would be done in relation to prohibitions contained in specific implementing Regulations issued under the Act.
Offences under the Regulations on DPRK (refer to paragraph 78 above)			

SECTION III – REGULATORY REQUIREMENTS

INTERNATIONAL REGULATORY REQUIREMENTS

57. The United Nations Convention Against Transnational Organized Crime and the Protocols Thereto, 2004 (Palermo Convention) established the following main obligations for member states of the United Nations:-

(a) Criminalization of participation in an organized criminal group;

(b) Criminalization of the laundering of the proceeds of crime;

(c) Measures to combat money laundering;

(d) Criminalization of corruption;

(e) Measures to address the liability of legal persons;

(f) Legal framework that adequately addresses, among other things,-
  (i) The prosecution and sanctioning of offences;
  (ii) Confiscation and seizure;
  (iii) International cooperation for purposes of confiscation;
  (iv) Extradition; and
  (v) Mutual legal assistance

58. The United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988 (Vienna Convention) established the following main obligations for member states of the United Nations:-

(a) Criminalization of the cultivation, production, sale, manufacture, transport or distribution of any narcotic drugs or psychotropic substances and the organization management or financing of any of these activities;

(b) Criminalization of the conversion or transfer of property knowing that the property was derived from any of the above mentioned activities for the purpose of concealing or disguising the illicit origin of the property;

(c) Criminalization of the concealment or disguise of the true nature, source, location, disposition, movement or ownership of property knowing that such property is derived from an offence or offences described at (a) or (b) above;

(d) Criminalization of activities ancillary to the commission of the offences at (a) – (c) above;

(e) Suppression of illicit traffic by sea in accordance with the international law of the sea;

(f) Adequate measures to suppress the illicit traffic in narcotic drugs, psychotropic substances and other substances in free trade zones and in free ports

(g) Adequate measures to suppress use of mail for the illicit traffic

(h) Legal framework that adequately addresses, among other things:-

(i) Sanctions that adequately take into account the grave nature of the offences;
(ii) Confiscation of the proceeds and instrumentalities of crime;
(iii) International cooperation for purposes of confiscation;
(iv) Extradition;
(v) Mutual legal assistance; and
(vi) Other forms of cooperation

59. The United Nations (U.N.) International Convention for the Suppression of the Financing of Terrorism 1999 established three main obligations for member states of the United Nations:-

(a) States must establish the offence of the financing of terrorist acts in their national legislation;

(b) States must engage in wide-ranging cooperation with other states and provide them with legal assistance in the matters covered by the Convention; and

(c) States must enact certain requirements concerning the role of financial institutions in the detection and reporting of evidence of the financing of terrorist acts.

Jamaica became a signatory to the U.N. International Convention for the Suppression of the Financing of Terrorism 1999 on November 10, 2000. On September 16, 2005 Jamaica deposited with the U.N., instruments of accession to /ratification of this Convention.

60. U.N. Resolution 1373 (2001) on threats to international peace and security caused by terrorist acts, also mandates all member states of the United Nations to take action against individuals, groups, organizations and their assets. As a consequence of the United Nation's characterization of acts of terrorism as threats to international peace and

security, the United Nations is entitled to take, if necessary, the collective measures ("sanctions") under Chapter VII of the United Nations Charter. [49] To this end the MFATF receives from time to time, an updated listing of individuals and entities which the UN has added to its consolidated list pertaining to Al-Qaida pursuant to United Nations Counter-Terrorism Security Council Resolution 1267 (1999) – Afghanistan. This listing is forwarded to the DPP for the purpose of being addressed pursuant to the listed entity regime. Licensees may, notwithstanding the foregoing, wish to apprise themselves directly from the United Nations web site and in that case may take note that the complete list and updates may be regularly accessed through the United Nations website.

61. The discussion above, at paragraphs 50-56, is also relevant for this section on the International Regulatory Requirements.

62. The Jamaican authorities are also guided by -

(a) The (2012) revised Forty Recommendations of the FATF on the Detection and Prevention of Money Laundering and Terrorist Financing.

(b) In October 2001, the Basel Committee on Banking Supervision issued Customer Due Diligence best practice standards ("CDD") as the minimum standards to be adopted by banking institutions in all countries. This document has been superceded by the Committee's publication of Sound Management of Risks Related to Money Laundering and Financing of Terrorism, issued in January 2014 and which can be accessed at the BIS website www.bis.org.

Other relevant publications published by Basel include -

(i) Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross Border Wire Transfers, May 2009 and

(ii) General Guide to Account Opening and Customer identification, February 2003.

[49] Suppressing the Financing of Terrorism – A Handbook for Legislative Drafting Chapter on U.N. Security Council Resolutions on Terrorism Financing - Page 15 – (Prepared by the IMF)

63. In conjunction with these Guidance Notes, financial institutions should be guided by the FATF standards, principles and recommendations in establishing policies, programs and procedures to prevent and detect money laundering and in combating the financing of terrorist activities as well as the prevention of the proliferation of weapons of mass destruction. The FATF Recommendations set out the internationally and regionally accepted principles relating to the appropriate measures to combat money-laundering, terrorist financing and the proliferation of weapons of mass destruction. The revised FATF Forty Recommendations can be accessed from both the FATF and CFATF[50] websites at www.fatf-gafi.org, and www.cfatf.org. Further guidance can also be obtained from the Best Practices issued by the FATF, which though not binding, outline very useful approaches to employ in addressing the international standards. Examples of some of the guidance issued by FATF and found on its website are listed below-

(a) Politically Exposed Persons, June 2013

(b) Combating the Abuse of Non-Profit Organisations, June 2013

(c) Guidance for a Risk Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services, June 2013

(d) The Implementation of Financial Provisions of UNSEC to Counter the Proliferation of Weapons of Mass Destruction, June 2013

(e) Targeted Financial Sanctions Related to Terrorism and Terrorist Financing, June 2013

(f) National Money Laundering Terrorist Financing Risk Assessment, February 2013

(g) Managing the AML/CFT Financing Policy Implications of Voluntary Tax Compliance Programmes, October 2012

(h) Combatting the Abuse of Alternative Remittance Systems, June 2003

(i) Risk Based Approach for Money Value Transfer Services, February 2016

[50] CFATF is a FATF Styled Regional Body (FSRB) comprising twenty-seven states of the Caribbean Basin, which have agreed to implement common countermeasures to address the problem of criminal money laundering. It was established as the result of meetings convened in Aruba in May 1990 and Jamaica in November 1992.

Advisories and Publications issued in relation to certain Jurisdictions

64. Public statements are issued by the FATF in relation to jurisdictions which have been identified as *Jurisdictions with either strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or which have not committed to an action plan developed with the FATF to address the deficiencies.* The FATF has therefore called on its members to consider the risks arising from the deficiencies associated with each of those jurisdictions.

These public statements are updated periodically can be accessed from the FATF's web site.

65. Public statements were issued by the CFATF in relation to three (3) of its members.[51]

These public statements are updated periodically can be accessed from the CFATF's web site.

Advisory by the Financial Stability Board

66. According to the Financial Stability Board ('FSB')[52], the publication of an advisory in relation to a jurisdiction comprises a negative measure that the FSB has agreed should be applied in relation to a jurisdiction that is considered to be a risk to the global financial system or which is non-compliant with international standards. An assessment of a jurisdiction's levels of compliance with regulatory and supervisory standards relevant to international cooperation and information exchange is based on assessments of underlying ROSCs[53] (prepared by the IMF and World Bank) as well as signatory status to the multilateral MOU overseen by IOSCO[54].

[51] At the time of preparation of the Guidance Notes, only one member remained subject to a public statement of this nature.

[52] FSB members – Australia, Argentina, Brazil, Canada, China, France, Germany, Hong Kong SAR, India, Indonesia, Italy, Japan, Korea, Mexico, Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Switzerland, Turkey, United Kingdom and United States.

[53] Report on Observance of Standards and Codes

[54] International Organization of Securities Commissions

Statutes Which May Impact Financial Institutions Doing Business in the United States of America ('US')

67. Although not falling within the ambit of international best practice, financial institutions with correspondent banking relationships in the US should also be aware of the USA Patriot Act, as well as the Foreign Narcotics Designation Kingpin Act and Regulations. These laws directly impact the offer of correspondent banking services by US financial institutions and their holding of assets overseas.

USA Patriot Act

68. The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ('USA PATRIOT') Act of 2001" - was passed by the US Congress in direct response to the September 11 terrorist attacks and became effective on 26 October 2001. This legislation has, among other things, expanded the money laundering laws of the US and has placed more stringent procedural requirements on financial institutions. Of specific importance to Jamaican financial institutions is the additional authority that has been vested in the US Secretary of the Treasury to regulate the activities of US financial institutions and in particular their relations with foreign individuals and entities. All banks and other financial institutions operating in Jamaica that have established correspondent accounts or any other business relationship with banks in the USA should therefore be aware of the provisions of this Act, including those highlighted below: -

(a) Provisions which permit the US Authorities to forfeit funds held by foreign banks in correspondent accounts held with banks situated in the US. (S. 319)[55]

(b) Provisions that will allow the US authorities to seize correspondent accounts held in US financial institutions for foreign banks which are in turn holding forfeitable assets. (s. 317 and s. 319)[56]

[55] Reference taken from "Current Developments in Monetary and Financial Law – Cap 19 – pages 349-352

[56] Reference taken from "Current Developments in Monetary and Financial Law – Cap 19 – pages 349-352.

(c) Provisions prohibiting US financial institutions from establishing, maintaining and administering or managing correspondent accounts with foreign banks that have no physical presence in any jurisdiction (i.e. shell banks), with certain limited exceptions; (s. 313)[57]

(d) Provisions requiring US financial institutions to take "reasonable steps" to ensure that accounts for foreign financial institutions are not used to indirectly provide banking services to shell banks; (s. 313)[58]

(e) Provisions which grant the Treasury and the US Attorney General power to issue a subpoena or summons to any foreign financial institutions with a correspondent account in the US and to request records relating to the account. A financial institution that has a correspondent account for a foreign financial institution must maintain certain delineated records in the US relating to that foreign financial institution; (s. 319 (b))[59]

(f) Provisions which grant the Treasury and the US Attorney General power to direct a financial institution to terminate its relationship with a foreign correspondent financial institution that has failed to comply with a subpoena or summons. The directive must be by written notice and non-complying financial institutions are subject to civil penalties of up to US$10,000 per day; (s. 319 (b))[60]

Foreign Narcotics Kingpin Designation Act[61]

69. 'Its purpose is to deny significant foreign narcotics traffickers, their related businesses, and their operatives access to the U.S. financial system and to prohibit all trade and transactions between the traffickers and U.S. companies and individuals. The Kingpin Act authorizes the President to take these actions when he determines that a foreign person plays a significant role in international narcotics trafficking. Congress modeled the Kingpin Act on the effective sanctions program that the Department of the Treasury's

[57] Ibid
[58] Ibid
[59] Ibid
[60] Reference taken from "Current Developments in Monetary and Financial Law – Cap 19 – pages 349-352.
[61] This update on the **Foreign Narcotics Kingpin Designation Act** is taken from White House Press Release, Office of the Press Secretary - April 15, 2009 - **Fact Sheet: Overview of the Foreign Narcotics Kingpin Designation Act**

Office of Foreign Assets Control[62] ('OFAC') administers against the Colombian drug cartels pursuant to Executive Order 12978 issued in October 1995 ("Executive Order 12978") under authority of the International Emergency Economic Powers Act ("IEEPA"). …

Under the Kingpin Act, the President may identify foreign entities as well as foreign individuals as Significant Foreign Narcotics Traffickers, or "kingpins": a foreign person is defined in the Act as "any citizen or national of a foreign state or any entity not organized under the laws of the United States, but does not include a foreign state." Likewise, the President is not required to designate Colombian persons exclusively under Executive Order 12978, and may impose sanctions on a Colombian individual or entity under the Kingpin Act, which is intended to be global in scope. …

Individuals who violate the Kingpin Act are subject to criminal penalties of up to 10 years in prison and/or fines pursuant to Title 18 of the U.S. Code. Entities that violate the Act face criminal penalties in the form of fines up to $10 million; officers, directors, or agents of an entity who knowingly participate in a violation of the Kingpin Act are subject to criminal penalties of up to 30 years in imprison and/or a $5 million fine. The Kingpin Act also provides for civil penalties of up to $1.075 million against individuals or entities that violate its provisions.'

US Executive Orders[63]

Iran Freedom and Counter Proliferation Act (IFCA), 2012

70. On June 3, 2013, the President issued Executive Order 13645[64] ("Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Freedom and Counter-Proliferation Act of 2012 and Additional Sanctions With Respect to Iran") ("E.O. 13645"). Section 2 of

[62] OFAC administers and enforces economic and trade sanctions based on US foreign policy and US national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific (US) legislation, to impose controls on transactions and freeze foreign assets under US jurisdiction" (Source - http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx

[63] Central Bank advisories on these Executive Orders were issued to financial institutions in July and August 2013

[64] This Order took effect on July 1, 2013

E.O. 13645 blocks, with certain exceptions, all property and interests in property that are in the United States, that hereafter come within the United States, or that are or hereafter come within the possession or control of any United States person, including any foreign branch, of persons determined by the Secretary of the Treasury, in consultation with the Secretary of State, to satisfy any of the criteria set forth in subsection (a)(i) or (a)(ii) of section 2.[65]

International Emergency Economic Powers Act (IEEPA), 2007

71. **US Executive Order 13581** of July 24, 2011 was issued by the President of the US in to the designation of persons pursuant to the International Emergency Economic Powers Act (IEEPA) (50 U.S.C. 1701 *et seq*.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq*.) (NEA), and section 301 of title 3, United States Code, **AND** in respect of which additional designations were made on June 5, 2013.

The Order authorizes the blocking of all property and interests that are in the US, that subsequently come within the US or that are or subsequently within the possession or control of any US person including any overseas branch of the persons listed in the Annex to the captioned order, and the persons determined by the Secretary of the Treasury to be a person to whom the Order applies (see targeted persons below) and further, that such property and interests may not be transferred, paid, exported, withdrawn or otherwise dealt in.

72. The Order accordingly targets –

(a) Any foreign person that constitutes a significant transnational criminal organization (TCO);

(b) Any person who has materially assisted, sponsored, or provided financial, material or technological support for, or goods or services to or in support of, any person whose property and interests in property are blocked pursuant to this Executive Order, and

(c) Any person who is owned or controlled by, or who has acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this Executive Order.

[65] Federal Register, The Daily Journal of the United States Government, https://www.federalregister.gov/articles/2014/09/05/2014-21169/actions-taken-pursuant-to-executive-order-13645 as at 28/8/15

73. For the purposes of this Order, the term "foreign person" means any citizen or national of a foreign state, or any entity organized under the laws of a foreign state or existing in a foreign state, including any such individual or entity who is also a US person; and the term "significant transnational criminal organization" means a group of persons, that includes one or more foreign persons which engages in an ongoing pattern of serious criminal activity involving the jurisdictions of at least two foreign states; and that threatens the national security, foreign policy or economy of the US.

US Economic Sanctions Programmes

74. OFAC administers a number of different sanctions programmes. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals[66].

As of November 2015, OFAC has in place sanction programs involving at least 20 nations, including Cuba, Crimea, Iran, Iraq, Lebanon, South Sudan, and Zimbabwe.

(a) **Specially Designated Nationals (SDN) and Blocked Persons**

OFAC has identified and officially "designated" numerous foreign agents and front organizations, as well as terrorists, terrorist organizations, and narcotics traffickers, on its SDN list, which contains over 5,000 variations on names of individuals, governmental entities, companies, and merchant vessels located around the world.

All U.S. persons (including individuals and organizations) are responsible for ensuring that they do not undertake a business dealing with an individual or entity on the SDN list. U.S. persons are:

(i) All U.S. citizens and permanent residents,

(ii) All persons located in the United States,

(iii) Overseas branches of U.S. companies, and

(iv) In the case of the Cuba and North Korea programs, non-U.S. subsidiaries of U.S. companies.

[66] http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx as at 11/11/15

A complete list of individuals and entities designated can be found at http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx

(b) **Penalties for Noncompliance**

The only way to assure compliance with OFAC-administered sanctions is to develop a process for regularly checking customers/clients against the SDN list described above. OFAC violations have serious consequences. Persons not complying with OFAC-administered sanctions are liable for significant penalties, even if their action was inadvertent or uninformed.[67] Penalties include:

(i) **Civil penalties**[68]**:** $250,000 or twice the amount of each underlying transaction up to $1,075,000 per violation
(ii) **Criminal penalties:** $50,000 to $10,000,000 fine; 10-30 years in prison
(iii) **Publication of penalty:** OFAC publishes the names of companies that have been penalized

DOMESTIC REGULATORY REQUIREMENTS

75. The domestic legal requirements outlined above at Section II of these Guidance Notes highlight the programmes, policies, procedures and controls for the purpose of preventing and detecting money laundering [69] terrorist financing[70] activities; and the proliferation of weapons of mass destruction activities which must be established and implemented by Financial institutions.

76. In summary, Financial institutions are expected to demonstrate full awareness of:-

[67] Recent actions of OFAC involving: Banks – USD16.562 million Settlement Agreement with BOA for apparent violations of the Foreign Narcotics Kingpin Sanctions Regulations, 31 C.F.R. Section 598; the Narcotics Trafficking Sanctions Regulations, 31 C.F.R. Section 536 (24/07/2014); and the Reporting, Procedures and Penalties Regulations, 31 C.F.R. Section 501; USD152 million agreement with Clearstream Banking, S.A. (Luxembourg) regarding an apparent violation of the Iranian Transactions and Sanctions Regulations, 31 C.F.R. Section 560 (23/01/2014).
[68] http://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx Gives a list of civil penalties and enforcement actions to date.
[69] See POCA (MLP) Regulations, 2007 (r. 5)
[70] See TPA section 18

(a) the nature of the money-laundering and terrorist financing threats, and the nature of threats of the proliferation of weapons of mass destruction;

(b) the local laws relating to combatting money-laundering, terrorist financing and the proliferation of weapons of mass destruction, and the potential liability of institutions and employees for failure to comply with these obligations; these Guidance Notes as well as related international standards and related best practices ~~(where available)~~;

(c) the obligations to ensure the implementation of the requisite systems for customer and ultimate beneficial ownership identification and verification, including special procedures for non-face to face transactions, electronic funds transfers transactions; high risk customers, 'Politically Exposed Persons' (PEPs), and transactions with overseas counterparts;

(d) the requisite systems for the recording and reporting of unusual and suspicious transactions and transactions that exceed the statutory thresholds; including the role of the nominated officer;

(e) the requisite programmes for ensuring employee integrity and awareness through effective screening and due diligence prior to hiring and continued relevant training post hiring, and continued screening of employees post hiring (viz. job performance; adherence to internal policies and procedures including codes of conduct and AML/CFT requirements as well as the general integrity of employees).

SECTION IV – RISK BASED FRAMEWORK

77. Under the revised FATF Forty (40) Recommendations, 2012[71] countries are required to identify, understand and assess, the money laundering and terrorist financing risks posed to the country. Based on that assessment countries must ensure that their national AML/CFT policies are informed by the risks identified. This national risk assessment will therefore inform the overall national AML/CFT strategy and framework for a

[71] FATF Recommendation 1 and Interpretive Note to Recommendation 1

country and the implementation of appropriate risk based measures for the relevant sectors within the country. The revised recommendations also indicate that the resulting national risk based approach employed by a country should not exempt financial institutions and Designated Non-Financial Businesses and Professions ('DNFBPs') from the requirement to apply enhanced measures when higher risk scenarios have been identified by these persons.

78. A financial institution shall identify, assess and take effective action to mitigate its money laundering and terrorist financing risks in relation to –

(a) Customers and other counterparts;
(b) Countries or geographic areas;
(c) Products;
(d) Services;
(e) Transactions;
(f) Delivery channels; and
(g) Operating environment (business (size, activities and complexities); sector; national and global issues)

A failure to carry out this requirement will constitute a breach of the BOJ's AML/CFT Supervisory Rules.

79. The assessment of risk as itemized above at paragraph 78 shall be:-

(a) undertaken on an ongoing basis to take account of new risks and changing circumstances and should therefore be undertaken periodically (at least once per quarter or more frequently depending on the circumstances) and assessments should be documented (i.e. "be in writing");
(b) undertaken so that there is a clear identification, determination and understanding of the risks involved;
(c) based on practical, comprehensive and up-to-date understanding of threats;
(d) include commensurate measures that are clearly defined and applied,

(e) approved by the Board or other body (by whatever name called) of the financial institution responsible for the governance and oversight of the financial institution, 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

(f) available to the internal and external auditors as well as the Competent Authority and Supervisory Authority.

Failure to comply with these requirements will constitute a breach of the BOJ's AML/CFT Supervisory Rules.

80. Assessments should be informed by a country's national risk assessment (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). However, the absence of a national risk assessment does not absolve a financial institution from undertaking its own assessment of the risks posed to its operations as reflected at paragraph 78.

81. In undertaking its assessment, where a higher risk scenario is identified a financial institution, shall apply enhanced measures to address such higher risks. A failure to carry out this requirement will constitute a breach of the BOJ's AML/CFT Supervisory Rules.

82. A financial institution should note that regardless of the level of risks involved, there is no exemption from recordkeeping requirements.

83. The BOJ's examination processes will continue to include an assessment of the adequacy of a financial institution's AML/CFT policies and systems, the institution's compliance with these policies and systems as well as the applicable legislation and these Guidance Notes. Accordingly, the AML/CFT oversight of licensees under the BSA by the BOJ is now undertaken through a specialized unit of the Supervisory Division which is tasked

specifically with the BOJ's AML/CFT oversight functions[72]. The objective of this approach is to:-

(a) assist with understanding each financial institution's AML/CFT risks;

(b) allow for a more targeted assessment of the adequacy and appropriateness of an institution's own risk assessments and AML/CFT policies and procedures, and

(c) facilitate the collection of data that will facilitate the BOJ's broader participation in the country's risk based assessment.

84. Financial institutions should be aware that as competent authority, the BOJ can have independent interaction with the designated authority or an authority of equivalent jurisdiction, regarding an institution's compliance with its obligations under the applicable legislation. A financial institution's breach of its obligations under the applicable legislation can, in addition to the imposition of sanctions, also be reported to the designated authority. (See paragraph 24 above on Competent Authority)

85. For licensees under the BSA, it is anticipated that the mandates at paragraphs 78 and 79, will be addressed through the group risk management initiatives that are contemplated by the consolidated supervisory provisions under the BSA[73]. A failure therefore to comply with these mandates may be considered to be a failure to manage group risks and may result in the BOJ taking regulatory action, under the BSA in addition to the sanctions that can be applied under the AML/CFT Supervisory Rules..

86. Where licensees under the BSA are required to provide information pursuant to parent company or holding company obligations to consolidate AML/CFT compliance initiatives, this can be done pursuant to paragraph (n) of the Ninth Schedule to that Act. Otherwise, the clearest option available to such a financial institution is to obtain the

[72] The decision to use this approach was taken in March 2015, an industry advisory was issued in April 2015.

[73] See Section XIV of the BSA

customer's consent to make the disclosure pursuant to the AML/CFT consolidated approach requirements.

Branches and Subsidiaries

87. Financial institutions are required to advise their branches/subsidiaries (resident in Jamaica or overseas)[74] of the provisions of the Jamaican AML/CFT laws together with the provisions of any applicable Guidance Notes insofar as the dealings of such subsidiaries or branches are affected. Branches are not considered to be legally distinct from their head office and therefore are subject to Jamaican laws.

88. Each financial institution is therefore required to assess the AML/CFT regime existing in any jurisdiction in which its branches and/or subsidiaries operate to ensure that its respective branches and subsidiaries apply the requirements of the Jamaican law. An exception is where the overseas operation is required to comply with the AML/CFT laws in that jurisdiction and those requirements meet or exceed Jamaican law. Where the AML/CFT requirements in that jurisdiction fall short of the Jamaican requirements[75] the financial institution should ensure that appropriate additional measures to manage the money laundering/terrorist financing risks are developed, documented, implemented and communicated to the BOJ.

89. Overseas based subsidiaries and foreign branches of local financial institutions must inform their local parent companies and local head offices if they are not in a position to observe AML/CFT measures of the local parent company or head office where compliance therewith will contravene the laws of the overseas jurisdiction/(s) in which these subsidiaries and branches reside. In such circumstances the local head office /parent company **must** accordingly advise BOJ[76], and ensure that, appropriate additional measures to manage the money laundering/ terrorist financing risks are developed,

[74] Regulation 18, POCA (MLP) Regulations, 2007 and Regulation 18 of the TP (Reporting Entities) Regulations, 2010
[75] Regulation 18 of the POCA (MLP) Regulations and FATF Recommendation 18
[76] See regulation 18(2) of the POCA (MLP) Regulations, 2007; and regulation 18(2) of the TP (Reporting Entities) Regulations, 2010

documented, implemented and communicated to the BOJ. BOJ will then make a determination on the adequacy of the measures applied and any other or further required course of action which may also include closure of the relevant overseas subsidiary or branch.

90. A Financial institution shall ensure that its local subsidiaries engaged in financial services implement, and conform to obligations under the POCA and under the TPA, and regulations issued thereunder as well as these Guidance Notes. A failure to carry out this requirement will constitute a breach of the BOJ's AML/CFT Supervisory Rules.

91. In complying with the mandates at paragraphs 78 and 79 a financial institution shall in relation to its subsidiaries and branches, ensure –

(a) the KYC details for customers are well documented (i.e. identification and other customer information as defined under the POCA (MLP) Regulations, 2007) is submitted and recorded); source of wealth is obtained as a part of the financial history of the customer as well as transaction details (including nature of the transaction, transaction amount; currency used; method of payment [cheque/cash/credit card/debit card/wire transfer] and source of funds used to make the payment) are recorded;

(b) AML/CFT internal regulatory controls (i.e. employee training; designation of a nominated officer; auditing of internal controls etc.) are documented (where applicable) and implemented;

(c) required disclosures (i.e. STRs) are made and any other reporting obligations are met.

(d) in relation to branch and subsidiary operations in Jamaica, measures that track cash transactions are to be implemented to prevent anonymity in relation to financing of transactions and source of funds. Additionally, financial institutions who are "permitted persons" as defined under POCA will need to invoke appropriate measures to ensure that where cash transactions over one million Jamaican dollars (or

the equivalent amount in any other currency) are facilitated, this does not itself facilitate a breach of the cash transaction limit provisions under POCA.

(e) AML/CFT risk based measures are employed within the parameters of the AML/CFT laws (eg. processes that include the imposition of transaction limits beyond or below which enhanced or reduced monitoring measures may be applied; or the application of measures commensurate with the risk profile of a customer or product etc.;).

A failure to carry out these requirements will constitute a breach of the BOJ's AML/CFT Supervisory Rules.

Non-Financial Subsidiaries

92. Licensees under the BSA are subject to mandates on the type of subsidiaries that can be held and must therefore always be in a position to prove to the BOJ that the operations and activities of their subsidiaries (especially where these are non-financial) are **relevant and complementary to the licensee**[77] and do not pose a financial drain or a money laundering or terrorist financing risk to the licensee.

The kind of AML/CFT processes implemented in relation to these types of subsidiaries should for practicality amount to measures designed to address the AML/CFT risks posed by these subsidiaries to their parent financial institutions.

93. Financial institutions that have local subsidiaries which are themselves subject to AML/CFT and other guidance from authorities other than the BOJ (whether regulatory or otherwise) shall assess the AML/CFT guidance against which their subsidiaries operate and shall ensure that those subsidiaries apply the higher required standard.[78] A failure to carry out this requirement will constitute a breach of the BOJ's AML/CFT Supervisory Rules. For licensees under the BSA this may also be considered to be a failure of the

[77] Section 73(2) BSA
[78] Regulation 18 of the POCA (MLP) Regulations , 2007; and regulation 18 of the TP (Reporting Entities) Regulations, 2010; See also FATF Recommendation 22

statutory obligation to manage group risks pursuant to the consolidated supervisory provisions under the BSA and could result in the BOJ taking other regulatory action.

Gatekeepers/Designated Non-Financial Businesses and Professions (DNFBPs) Affiliates and Counterparts

94. According to FATF persons falling within the definition of 'Designated Non-Financial Businesses and Professions (DNFBPs) comprise - lawyers, notaries, other independent professionals[79] and accountants; dealers in precious metals and stones (jewelers); trust and company service providers; casinos; and real estate agents) (See FATF Recommendation 22 and the Interpretative Notes thereto). The FATF Recommendations also state that (in the situations outlined in the recommendations) such persons should be subject to the following:-

(a) Implementation of AML/CFT regulatory controls (policies and procedures including training of employees and audits of AML/CFT controls (FATF Recommendation 18);

(b) The customer due diligence and record-keeping requirements set out in recommendations 10 (customer due diligence), 11 (record keeping), 12 (politically exposed persons), 15 (new technologies) and 17 (reliance on third parties);

(c) Suspicious Transaction Reporting (STR) requirements (FATF Recommendation 20) and as such entitled to protection from any liability from such disclosures made and prohibited from disclosing the fact of the STR or related information being reported to the designated authority (FATF Recommendation 21, and

(d) Requirements for other measures such as internal controls and foreign branches and subsidiaries obligations (R 18); and obligations regarding higher risk countries (R19).

[79] In November 2014 the Bar Association obtained an interim remedy in the form of an injunction from the court preventing the operation of the regime as it applies to lawyers on condition that a Hearing for seven days commencing not later than February 02, 2015 has been set for the matter to be heard regarding the constitutionality of the law.

Financial institutions should therefore take the matters set out in this paragraph and below into consideration when establishing or in the course of maintaining a relationship with a designated non-financial business.

95. The POCA is applicable to business in the regulated sector. A business is in the regulated sector if it is a financial institution or an entity that has corporate responsibility for the development and implementation of group wide anti-money laundering or terrorism prevention, policies and procedures for the group of companies of which the entity forms a part; or a designated non-financial institution ('DNFI')[80]. A means "…*a person who is* –

(i) Not primarily engaged in carrying on a financial business; and

(ii) Designated as a non-financial institution for the purposes of this Act by the Minister by order subject to affirmative resolution."

A DNFI is therefore subject to the statutory AML provisions that are applicable to financial institutions.

96. In November 2013, the following persons were designated by the Minister of National Security as DNFIs - real estate dealers, casinos, gaming machine operators, lawyers, notaries, other independent legal professionals and accountants, in relation to the activities specified in the designation orders[81]. (Refer to Appendix III for copies of the requisite Designation Orders)

[80] Refer POCA, 2007 Fourth Schedule as amended and paragraph 16 of the Proceeds of Crime (Amendment) Act, 2013

[81] The Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order, 2013; (effective April 2014)
The Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order, 2013; (effective April 2014)
The Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order, 2013; (effective June 2014)
The Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order, 2013; (effective April 2014)
The Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013; (effective April 2014)

(a) The designated Competent Authorities[82] for these persons are-

The Real Estate Board (re: Real Estate Dealers)
The Betting Gaming and Lotteries Commission (re: Gaming Operators)
The Casino Commission (re: Casinos)
The General Legal Council (re: Attorneys)
The Public Accountancy Board (re: Accountants)

(b) In October 2013, amendments were passed to the POCA to, among other things, incorporate provisions that would further facilitate the implementation of an oversight framework for DNFIs in Jamaica. Accordingly, section 91A accords more explicit powers to the Competent Authorities (i.e. supervisors/regulators) for the Regulated Sector (both financial institutions and designated non-financial institutions) as follows:

(i) to carry out inspection/verification exercises (directly or through a 3rd Party);
(ii) to issue directions to ensure compliance with the statutory requirements;
(iii) to examine and take copies of documents;
(iv) to share information on findings from regulator to regulator or the FID (not including protected information[83])
(v) to impose a requirement (if none exists) for registration of persons with such particulars that may be prescribed.
(vi) to impose requirements for reporting to the Competent Authority.

(c) Subsection (3) of section 91A reflects that the obligation to allow the Competent Authority access to information of the DNFIs is subject to legal professional privilege. However subsection (4) makes it clear that this exemption for legal professional privilege does not apply to information or other matter that is communicated or given with the intention of furthering a criminal purpose.

(d) Subsection 6 of section 91A provides for penalties that will be applicable on conviction for failing to comply with a requirement or directive from the Competent Authority, which may be both criminal (fine not exceeding JMD$250,000 on conviction in the RM Court and fine not exceeding JMD$1m on conviction in the Circuit Court) and administrative (such as the revocation of an operating licence).

[82] Designations took effect November 29, 2013.
[83] Information that is protected from disclosure under the POCA or under any other Act – s.91A(2)(d)(i) POCA

97. It should also be noted where the DNFI makes a disclosure it is protected under the POCA, from the disclosure being interpreted as a breach of information restraints to which that DNFI may have been subject. Accordingly, section 100 states that -

(a) Once the information or matter comes to a person in the course of that person's trade, profession, business or employment; and

(b) that information or matter raises the belief or knowledge that another person has engaged in money laundering; and

(c) the disclosure of the information or matter is made to an authorized officer (i.e. a constable; a customs officer; or an officer of the Asset Recovery Agency) or a nominated officer;

such disclosures shall not amount to a breach of any restriction on the disclosure of information by whatever means imposed.

SECTION V – "KNOW YOUR CUSTOMER" (KYC) "KNOW THE TRANSACTION COUNTERPARTY" "CUSTOMER DUE DILIGENCE" (CDD)

Interpretation

98. For the purpose of this section of the Guidance Notes, the terms used in this section will have the meaning set out in this paragraph.

"affiliate" has the meaning assigned in section 2 of the Companies Act;

"charity/charities" means charitable organization as defined in section 2 of the Charities Act, 2013. For the purpose of these Guidance Notes the term 'charity' includes a non-profit organization (NPO);

"connected Party" has the meaning assigned in the Banking Services Act;

"current" in relation to information means information which is valid in substance, and accurate in respect of all [material] details and particulars;

"customer name" means,

(a) in the case of a natural person, the official name recorded at birth or recorded in the records of the Deputy Keeper of the Records and verified by sight of the official identification document as described in paragraph 121 below;

(b) in the case of a legal person, the name in which the business is incorporated or established, and verified by sight of the certificate of incorporation or certificate of Registration of Business Name;

"known employer" means :-

(a) in the case of a business, one that is registered on the Jamaica Stock Exchange; with a medium or small enterprise (MSME) which is registered with the Development Bank of Jamaica as an 'on-lender of funds';

(b) a financial institution as defined in these Guidance Notes;

(c) a financial institution which is registered with or licensed by the Financial Services Commission; or

(d) an employer within the public sector. Public sector for the purposes of these Guidance Notes means the Central Government or a public body[84] as defined in the Financial Administration and Audit Act;

"long standing customer" means a customer with which

(a) a business relationship is held by the financial institution and in respect of which, such relationship was established prior to the 29th day of March, 2007; and

(b) in respect of which there has been no change in the risk profile of that customer;

"non-profit organization" see 'charity' above;

"outdated information" refers to information other than current information and accordingly includes:-

(a) expired identification, (i.e. identification where the validity of the identification has ended or has expired);

(b) In relation to the name of a customer, a change of name of the customer, subsequent to the date when the customer commenced the business relationship with the financial institution or since the date the last transaction was conducted with the financial institution (whether or not the transaction was conducted at the same branch location).

(c) In relation to a customer's residential address (in the case of a natural person) or registered address (in the case of a legal

[84] "public body" means a statutory body or authority or any government company; (section 2 –the Financial Administration and Audit Act)

person), the address at which the customer no longer physically resides or is no longer physically situated;

(d) In relation to financial and other information regarding the personal, business or official affairs of the customer,

(i) (for financial information) the date at which the information represented has expired for at least 18 months, **or**

(ii) information in respect of which an intervening event has occurred after the information is provided to the financial institution and which event makes the information provided, unreliable or unhelpful for the institution to undertake its know your customer and customer due diligence and risk profile analyses;

"ongoing measure" means, in relation to a customer or transaction, a measure that must be applied by a financial institution for the duration of the business relationship or when a transaction is conducted in the course of the institution's business;

"personal or private Information" means, in relation to:-

(a) A natural person, customer information as defined in regulation 7(5) of the POC (MLP) Regulations;

(b) A legal person, the information set out in regulation 13(1)(c) of the POC (MLP) Regulations and at regulation 13(1)(c) of the TP (Reporting Entities) Regulations;

"records" includes records pertaining to identification, transactions, business correspondence, accounts files, instructions, determinations and bases for allowing or not proceeding with a transaction; account reviews and findings, transaction reviews and findings, requests for updated CDD or KYC information and related updates provided, accessed or ascertained);

"repeat customer" means, a person who transacts business of US$250 and over or the equivalent amount in any other currency more than once with the

financial institution or any of its branches, [subsidiaries or other connected parties or affiliates] within a three month period;

Comment [CM1]: Words in square bracket for review on whether their effect extends the concept of 'repeat customer' too widely.

"senior officer" for the purposes of this section of the Guidance Notes, in relation to –

(i) a body corporate, means an executive director, a managing director, a chief executive officer, a chief financial officer, the nominated officer, a manager and the company secretary or such other person by whatever name called, who undertakes duties of has responsibilities akin to these positions;

(ii) any other legal arrangement, includes an individual whose function, by whatever title used, involves functioning as an executive director, a managing director, a chief executive officer, a chief financial officer, a nominated officer, a manager or a company secretary or such other function by whatever name called which is akin or equivalent to these functions;

"significant transaction" means a transaction undertaken by a financial institution in respect of a customer, which varies substantially in value and/or in amount of business conducted or number of transactions normally undertaken by that customer or in relation to the account/(s) involved. For instance,

(a) an account ordinarily involving low value JMD transactions suddenly being used for mid-to-high value transactions in JMD or foreign currency;

(b) a relationship that is normally related to banking activities for a corporate customer is used to finance or cover personal expenses or conduct personal banking activities;

(c) or deposit and withdrawal activities consistent with a standard personal savings account becomes more consistent with those indicative of flows generated from and/or expenses associated with commercial activity.

General Requirements for Know Your Customer ("KYC") & Customer Due Diligence ("CDD")[85]

99. The requirement to 'know your customer' involves satisfactorily identifying the customer and satisfactorily establishing details pertaining to the customers' identity, occupation, economic activity, personal financial track record, business track record, source of wealth , source of funds that will be involved in the transaction, contact information and details, capacity in which the business is being transacted, details of representation relationship, authorities established to act for persons benefitting from the transaction or relationship with the financial institution, regulatory status (i.e. compliance record with statutory and operational obligations), personal compliance with laws (i.e. character and integrity).

100. The requirement to conduct customer due diligence involves identifying the customer and verifying that customer's identity. In the case of customers which are legal persons or established by some other form of legal arrangement, identification of the customer includes identification of the beneficial owner/(s) and verifying that identification[86]. The customer due diligence that is conducted must be designed to allow a financial institution to understand who its customers are by requiring the gathering of information on what the customer does and why that customer requires the services requested of the financial institution[87]. Where the customer is a legal person or established by legal arrangement the due diligence undertaken should include understanding the ownership and control structure of that customer[88].

Policies and Procedures

101. Central to an effective anti-money laundering and anti-terrorist financing programme is the formulation and implementation of comprehensive, rigorous and thorough customer due diligence and KYC policies and procedures.

[85] See POCA (MLP) Regulations, 2007 (r. 7, 11, 12, 13); TP (Reporting Entities) Regulations, 2010 (r. 7, 11, 12, 13); and FATF Recommendations R.10
[86] FATF Recommendation 10 (CDD measures to be taken)
[87] FATF Risk Based Approach Guidance for the Banking Sector, October 2014 – Section III B – Risk Mitigation
[88] FATF Recommendation 10 (CDD measures to be taken)

KYC policies and procedures must contain a clear statement of management's overall expectations and establish specific lines of responsibilities not only at the point of the institution's first contact with the customer, but throughout the business relationship. Policies and procedures must be properly documented and clearly communicated and readily available to staff.

KYC policies and procedures should not only be geared toward the timely prevention and detection of money laundering and terrorism financing activities, but must also form a fundamental part of the financial institution's overall risk management and internal control systems. This is essential, as inadequate KYC standards can result in undue risk exposures, particularly as they relate to ML/FT, reputational, operational, legal and concentration risks.

102. Policies and procedures must therefore be developed on the basis of the financial institution's risk assessment/(s) and should therefore be reflective of[89]:-

(a) The financial institution's understanding of the ML/TF risks present in its customer base, delivery channels, products and services offered, and under development before these are launched as well as the jurisdictions within which the FI or its customers do business.

(b) The financial institution's understanding of risks present in its general operations, which could impact or increase its exposure to a ML or TF related offence taking place, for example, risks associated with product usage; transaction patterns, group of accounts or a particular category of customers; inadequate internal control mechanisms, weak hiring policies, absence of appropriate and periodic AML/CFT training for the board, management and staff; weak communication policies, absence of clear reporting lines and responsibilities within the financial institution; weak disciplinary mechanisms (in terms of sanctions and/or appropriate remedial

[89] Reference: Basel Committee on Banking Supervision – Sound Management of Risks Related to Money Laundering and Financing of Terrorism – January 2014

measures/mechanisms); lack of access to timely information, poor records management practices and weak records management and retention policies; absence of robust escalation of matters to the Board's attention; ineffective compliance functions.

(c) Threats and vulnerabilities that have been identified which have a probability of occurring and the impact such occurrences could have on the FI's operations and reputation.

(d) Customer and transaction acceptance requirements which should be informed by an assessment of the types of customers that are likely to pose a higher risk of ML or TF or lower risk of ML or TF. Accordingly, while basic due diligence is applicable to all customers and transacting counterparties, policies and procedures should clearly reflect the due diligence that will be applicable for relationships or transactions that are subject to assessments of risks assessed as low, medium or high.

(e) Circumstances in which transactions can be started or business relationships established prior to verification of the CDD or KYC information.[90]

(f) Circumstances in which transactions or relationships can, should or must be terminated or discontinued, circumstances in which relationships will not be established and transactions will not be conducted or facilitated.

(g) Bases on which risk profiles for customers, products, delivery channels or services offered can be revised and the procedure for such revision. In this regard financial institutions should develop graduated "know your customer" policies and procedures for high-risk customers that go beyond the basic information-gathering requirements for average/low risk clients. This would include a detailed description of the types of customers that are likely to pose a higher than average risk to a financial institution

[90] POC (MLP) Regulations, 2007 regulation 13(2); TP (Reporting Entities) Regulations, 2010 regulation 13(2)

based on assessment of certain factors including customers' background, country of origin, important public or high profile position/(s) held, linked accounts, business activities or other risk indicators.

(h) Measures designed to allow for the identification of high risk customers and transactions in relation to the proliferation of weapons of mass destruction obligations as required by the UNSCRIA and regulations thereunder.

103. Accordingly, the minimum, KYC policies and procedures shall address: -

(a) The identification of the customer and the interim and ultimate beneficial owners or beneficiaries thereof, verification of such identification information, and the ascertainment and verification of the nature and purpose of a customer's business in order for the financial institution to have a basis for assessing the risk profile of the transaction or business relationship[91], and for determining whether a transaction is unusual or suspicious, or fits the norm expected of such a business;

(b) Accessing, obtaining and verifying the customer's personal information as well as the customer's financial history, source of wealth, source of funds for the transaction to be conducted, objective and purpose for requiring the financial service – including whether this is for personal, commercial or official use and establishing whether the customer is acting in his own right or on behalf of another; details of the commercial or official business where purpose for requiring the service is indicated as being for commercial or official business.

(c) The recording and regular review of customer information (identification and other information) as well as transaction information/records to ensure that the information kept by the financial institution is current 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

[91] POC (MLP) Regulations, 2007 (Amended 2013) reg. 7A

terminated. Under the POC (MLP) Regulations, financial institutions are required to ensure that customer information is kept under review with a view to ensuring its accuracy and is updated at least once every seven years or, at more frequent intervals as warranted by the risk profile of the relationship. If therefore during the course of the business relationship an institution's records reflect that the customer's information is outdated, the institution should update that information at the earliest opportunity as the KYC/CDD process is an ongoing measure;

(d) The application of KYC due diligence which take account of the level of risk posed to the financial institution by transacting business with the particular customer; (i.e. individuals opening standard savings accounts obviously funded primarily by salary; pension payments etc. vis-à-vis corporate accounts opened via pooled arrangements involving multiple parties or accounts for customers.);

(e) Measures clearly reflecting that accounts for high-risk customers must not be opened unless senior management approval is obtained[92].

(f) Mechanisms designed to ensure that there are adequate management information systems to provide timely and comprehensive management reports to facilitate effective monitoring of high-risk client accounts by senior management.

(g) Measures to deal with special areas of operations or operational complexities (eg. financial institutions which have established operations (via branches and subsidiaries) in more than one jurisdiction; or financial institutions within a financial group which offers a wide range of financial products and services; or financial institutions with a very diverse customer base).

[92] Whilst the term senior officer in these Guidance Notes includes a Nominated officer, a Nominated officer is ineligible as a senior manager who can extend such approvals as such a function is to be sufficiently independent of the business line of the institution to allow for an objective assessment, monitoring, and enforcement of the institution's compliance with its AML/CFT obligations (legislative; as well as policies and procedures). (See also Part VI of these Guidance Notes)

104. A failure to carry out any one or more of the requirements in paragraph 103 will constitute a breach of the BOJ's AML/CFT Supervisory Rules.

105. Policies and procedures must be approved by the Board of directors (or other body by whatever name called) of the financial institution. Noncompliance with this requirement will constitute a breach of the Supervisory AML/CFT Rules.

106. For licensees under the BSA, it is expected that CDD procedures will also be applied on a consolidated and global basis where applicable. This requires inter alia, the capacity to aggregate and monitor significant balances and transactions for the under-mentioned customers:

(a) Customers with multiple accounts/transactions at the financial institution - either within a particular branch or among several branches situated within the local and foreign jurisdiction; and

(b) Customers with multiple accounts/transactions at several entities within the financial group.

This is required whether the accounts are held on balance sheet, or off-balance sheet as assets under management, [93] or on a fiduciary basis.

107. Vulnerability is not limited to transactions with customers. Any transaction undertaken by the financial institution can expose that institution to AML/CFT, reputational, operational, legal and/or concentration risk. As far as is reasonably practical and possible, financial institutions should apply the KYC policies and procedures to **all financial transactions undertaken whether customer related or not.** For these purposes, non-customer related transactions include: –

[93] Reference herein to assets under management is only to the extent that deposit taking institutions have their own assets under proprietary management Otherwise, asset management on behalf of customers is not an activity that can legally be undertaken by deposit-taking institutions. See also BSA section 54.

(a) Transactions conducted by the financial institution on its own behalf or on behalf of another financial institution; and

(b) In-house operational matters (proprietary securities acquisitions or dispositions; correspondent (local and overseas) relationships; housekeeping matters; administrative matters and so forth).

BANKS, MERCHANT BANKS, BUILDING SOCIETIES, CREDIT UNIONS, CAMBIOS AND REMITTANCE COMPANIES

General Requirements for Know Your Customer ("KYC") & Customer Due Diligence ("CDD")[94]

108. A business relationship or one-off transaction must not be established or continued until the identity of the customer (i.e. all CDD requirements), and the customer's 'know your customer' particulars are satisfactorily determined[95] (if this information is not already with the financial institution in the case of existing relationships or accounts), and the customer clearly indicates the capacity in respect of which the relationship or transaction with the financial institution is being established or undertaken. Accordingly, where an applicant for business refuses to produce any requested information, the relationship **must not** commence or the transaction **should not** proceed. Where an existing customer unreasonably refuses to provide the information requested by the financial institution pursuant to CDD or KYC requirements, or if any other verification problems arise which cannot be resolved, the business relationship with that customer should be legally terminated (unless otherwise advised by law enforcement authorities.

[94] See POCA (MLP) Regulations, 2007 (r. 7, 11, 12, 13); See TP (Reporting Entities) Regulations, 2010 (r. 7, 11, 12, 13); and FATF Recommendations R.10

[95] See POCA (MLP) Regulations, 2007 (r.7and 19); See TP (Reporting Entities) Regulations, 2010 (r. 5 and 21);

109. In seeking to –

(a) discontinue the procedures for establishing a business relationship or the transaction started or attempted; or

(b) terminate the business relationship,

financial institutions should be mindful of the prohibition against tipping off or unauthorised disclosures outlined under sections 97 and 104 POCA and section 17 of the TPA respectively and should therefore be careful not to "tip off" applicants for business, customers, or any other person where a suspicion has been formed by the financial institution that an offence is being attempted or has been or is being committed[96].

110. Financial Institutions should ensure that they have the ability to legally terminate arrangements, transactions or the business relationship, where the financial institutions form the view that criminal activity is taking place and that continuing the arrangement, transaction or relationship could lead to legal or reputational risks to the institution due to the suspected criminal activity.

Financial institutions must therefore ensure that their mandates with customers and indeed contractual arrangements entered into in the course of the regulated business permit the legal termination of the arrangement, transaction, or business relationship, in the event the view is formed that criminal activity is taking place and to continue with the arrangement, transaction or relationship would expose those institutions to legal or reputational risks due to the suspected criminal activity.

Mandates that do not allow for such termination and in respect of which the related accounts present immediate ML/FT risks should be reported to the designated authority and the institution should obtain legal advice on how to proceed. As regards termination without

[96] *Shah v HSBC Private Bank (UK) Ltd (No 2) [2012] EWHC 1283(QB)*, the ruling confirms that to ensure distance from the zone of 'tipping-off', a money laundering reporting officer should stay clear of any dialogue, with the customer, about the fact that a report was made under POCA to the requisite statutory body. This appears to be the current legal position, it remains to be challenged in the Court of Appeal.

tipping off, institutions may also need to consider consulting with the designated authority on this issue.

111. Financial institutions should undertake regular reviews[97] of all existing customers' records (identification & other particulars) to ensure that they remain up-to-date, relevant, consistent with the financial institution's risk profile of that customer, and remain subject to appropriate know your customer and customer due diligence processes. These reviews should be done **at least** seven years from the date of the commencement of the relationship and at minimum seven years increments thereafter, or, at more frequent intervals to ensure the accuracy of the information held by the institution or as warranted by the risk profile of the relationship.

112. The documentation provided to establish the relationship with the financial institution should be continually reviewed and updated. The customer is obligated to notify the financial institution of any change in identification information or changes in other particulars whether personal or private information or otherwise which would render the information with the financial institution to be outdated.

113. Reviews[98] would also be necessary under the following circumstances: -

(a) Upon the execution (or attempted execution) of a significant transaction;
(b) Upon material changes to customer documentation standards;
(c) When there is material change in the manner in which the account is operated;
(d) When, during the course of the business relationship, doubt arises regarding the true identity of the customer or the beneficial owner of the account;
(e) When there is any change in the ownership or control of a corporate customer, or of a customer established through a legal arrangement;

[97] POCA (MLP) Regulations, 2007 - r. 7(1)(c)&(d) and r. 19; TP (Reporting Entities) Regulations, 2010 (r. 5 and 21)

[98] POCA (MLP) Regulations, 2007 – r. 7(2)(b) and 7(3); and TP (Reporting Entities) Regulations, 2010 – regulations 5 and 6(2)(b)).

(f) Where the financial institution becomes aware at anytime that it lacks sufficient information about an existing customer/or about the existing business relationship with a customer;

(g) Where any transaction involves /exceeds the prescribed amount and represents a significant transaction or a material change in the manner in which the account is operated[99];

(h) Where transactions carried out in a single operation or in several operations appear to be linked;

(i) Where a transaction is carried out by means of wire transfers;

(j) Where there is any doubt about the veracity or adequacy of previously obtained evidence of identity;

(k) Where the financial institution is required to make a report under section 94 (STR) or 95 (STR by the nominated officer) of the POCA, or under section 16(3) or (3A) of the TPA (STR by the nominated officer – TP (Reporting Entities) Regulations, regulation 15)[100].

114. If during the course of the updating exercise or anytime after the business relationship has commenced the financial institution discovers that the information on file is not accurate, or is no longer applicable and the correct or updated information is not available or is, in the view of the financial institution, unreasonably withheld then the financial institution must take steps to terminate the relationship[101] and should consider referring the matter to the Designated Authority. The financial institution should conduct the necessary analysis and review of the account to inform its consideration of whether the matter should be referred to the Designated Authority[102] and records of the conduct and results of this exercise should be in writing and available on request, to the competent authority, and the

[99]POCA speaks to the following prescribed amounts - a TTR limit for cash transactions (see regulation 3 of the POC (MLP) Regulations and cash transaction limits (see POCA section 101A). No amounts are prescribed under the TPA or regulations thereunder.

[100] Financial institutions should be guided by their respective statutory AML/CFT obligations and where the circumstances call for this, the transaction should either not be conducted or consideration be given to terminating the relationship.

[101] POC (MLP) Regulations, 2007 regulation 7(1)(b) & TP (Reporting Entities) Regulations, 2010 regulation 5(a)(iii)

[102] POC (MLP) Regulations, 2007 regulation 7(1)(b)

Designated Authority within the time indicated in the request[103], and should also be available to the auditors (internal and external) where applicable, of that institution. In such cases those accounts should be legally terminated unless a direction/request to the contrary is received from the Designated Authority.

Unclaimed Moneys[104]

115. If the circumstances described above occur in the case of accounts that would qualify as unclaimed monies then, subject to any contrary directives from the Designated Authority pursuant to the appropriate consent requirements, on closure of the account, the funds contained therein should be subject to the usual course of action governing unclaimed moneys.

Other Accounts

116. If the circumstances described above occur in the case of accounts that would not qualify as unclaimed monies, then, subject to any contrary directives from the Designated Authority pursuant to the appropriate consent requirements, on closure of these accounts the funds contained therein should be returned to the named account holders.

Updating KYC Records

117. The law requires that KYC/CDD information be updated at a frequency of at least once every seven (7) years[105] from the date of the commencement of the relationship and at minimum seven year increments thereafter, or, at more frequent intervals to ensure the accuracy of the information held by the institution or as warranted by the risk profile of the relationship.

[103] Regulation 14(4) of the POC Regulations amended 2013 (NB. Regulation 14 of the TP (Reporting Entities) Regulations speaks to the record keeping obligation of reporting entities).
[104] Section 126 BSA. The concept of unclaimed balances is not applicable to credit unions and building societies.
[105] POC (MLP) Regulations, Regulation 7(1)(c) & (d),19

Where gaps are discovered in the KYC database[106] financial institutions must ensure that these gaps are addressed at the earliest opportunity and not at the end of a 7 year period from the last update. Updates in this regard would include matters involving-

(a) Addressing omissions in the database of KYC information particulars that are required under the law or AML/CFT regulatory framework (particularly where this occurs in relation to customers that are identified or classified as 'high risk');

(b) Addressing incomplete information. (If for instance the customer provided an alias or trading name other than the customer name as defined in these Guidance Notes, then the information on the institution's database should be treated as incomplete and the customer name must be obtained and verified);

(c) Adjusting records to reflect changes to the KYC particulars such as, name change by marriage or deed poll; changes in the current permanent address; changes in employment/business trade and/or profession; identification updates (Drivers Licences expire every 5 years; Passports expire every 10 years etc.) financial institutions should ensure that the records reflect the appropriate updates in this regard (i.e. current information);

(d) Correcting errors or addressing inaccuracies.

The KYC processes should ideally be implemented in a manner designed to minimize the disruption of business, accordingly the requirements need not be 'sprung' on existing customers. Such persons may for instance be provided advance notification of the information required and given a reasonable timeframe within which to provide the information. For example in the case of existing customers wishing to do new business with the bank, this would be an appropriate time to seek to ensure KYC updates and shortfalls are addressed.

[106] The law indicates there is no obligation for such reviews to be done in relation to matters which pre-date the prescribed date of 29th day of March 2007 (regulation 19(3) – POC (MLP) Regulations amended 2013.

References

118. In the case of customers other than long standing customers, these persons are subject to the requirement for 2 references however one of these references can be provided by a Senior Officer within the financial institution at the location with which the relationship has been established and who has personal knowledge of the customer; (that is to say, that Officer must himself or herself know the customer from direct personal contact with the customer over a period of time and in such a manner that allows for that Officer to truthfully attest to knowing the customer. A passing association with the customer, or knowledge of the customer which knowledge is gained from a source other than direct personal contact over an extended period of time or an immediate relative, would not suffice and will be interpreted accordingly for the purposes of these Guidance Notes). The other reference must however be obtained from an independent third party. The requirement of 'independence' requires the absence of any familial relationship and the absence of the existence of any vested interest in the acceptability of the reference.

Natural Persons

119. Financial institutions should be aware that the best identification documents for natural persons are those that are the most difficult to obtain illicitly. Positive identification must be obtained from documents issued by reputable sources[107] which include any one of the following:

(a) valid driver's licence (bearing a photograph), issued by the authorities in the country in which the person is resident".

(b) current valid passport (bearing a recent photograph);

(c) current valid voter's identification card with a recent photograph;

(d) signed (known) employer identity card or worker's identification from a known employer, bearing a photograph and signature of the worker in question and bearing the authorized signature on behalf of the employer;

[107] See Basel Committee on Banking Supervision – Sound management of risks related to money laundering and financing of terrorism, January 2014 paragraph 37

120. In cases where the identification described at paragraph 119 above genuinely cannot be produced, the financial institution will need to analyse the situation to determine whether it should exercise its discretion to facilitate the transaction on the basis of alternative forms of identification.

121. The acceptable forms of alternative identification include, in the case of:-

(a) an applicant for business, a birth certificate (or equivalent document of constituting a jurisdiction's official record of birth) accompanied by a Voluntary Declaration of Identification (or equivalent document with equivalent attestation requirements) from a person who is personally familiar with the subject of the Declaration and which has a familial relationship with the subject (i.e. parent, guardian or older sibling etc.) and a photograph both of which (i.e. the Declaration and the photograph) must be signed by any one of the following-

(i) Justice of the Peace (JP),

(ii) Notary Public, or

(iii)Attorney-at-Law,

to whom the customer is personally known for a period of not less than twelve months, and who is reasonably capable of confirming the identity of the customer;

(b) a customer or applicant for business who has not attained the age of majority[108], and who is enrolled in a secondary or tertiary institution, a valid school ID may be accepted **PROVIDED**:

(i) The ID has the following features:

1. A photograph of the student
2. Signature of ID holder (student)
3. ID Number

[108] See The Law Reform (Age of Majority) Act, 1979, sections 3 and 6

4. Expiry date of ID

5. Name of the relevant academic institution (high/secondary school or tertiary institution

6. Signature of principal/bursar/vice-principal of the relevant academic institution.

(The foregoing is applicable only to individuals under the age of 18 years as persons over 18 years of age will have attained the age of majority and will have achieved the age limit to qualify for obtaining other forms of identification i.e. Drivers Licence; Voters I.D. etc..); and

(ii) The transaction pertains to the opening of an account through or with at least one adult constituting either the parent or legal Guardian of the applicant for business; or the transaction pertains to an account that is held jointly with at least one adult constituting either the parent or legal Guardian of the customer.

122. Where a financial institution is approached for business by a person seeking to use an acceptable form of alternative of identification, the financial institution

(a) must be satisfied that:- the person's inability to produce at least one form of standard identification (as listed in paragraph 119 above) is genuine; and

(b) must ensure that appropriate safeguards are in place consistent with the assessed risk profile of the customer such as, transaction threshold limits applied to the business transacted.

123. It is not anticipated that a significant portion of the customer base of a financial institution will fall within this category. Consequently, a financial institution that seeks to rely on this exception above as the normal acceptable form of identification outside of the parameters indicated at paragraph 119 will be deemed to be acting contrary to its KYC/CDD obligations and will expose itself to regulatory action.

124. Paragraphs 120-122 outline minimum requirements a financial institution should address when approached by applicants for business who seek to transact business using alternative forms of identification. However a financial institution's KYC processes and procedures (see paragraph 105) should also speak to this matter and should clearly indicate the transaction safeguards and other measures that will be applied to minimise the risk of conducting business with a person using an alternative form of identification.

125. KYC details for natural persons that must be in place for basic KYC requirements **and** in the event the financial institution is served with a customer information order include the following[109]:-

(a) Information below in paragraph 126;
(b) Account / transaction number;
(c) Date on which the individual began to hold the account;
(d) Date on which the individual ceased to hold the account;
(e) Transaction date and description of transaction type;
(f) Account number of any other accounts to which the individual is a signatory and details (comprising the personal or private information) of the other persons holding those accounts;
(g) Source of funds that will be used in the transaction or used to access the service offered by the financial institution;
(h) Source of wealth;
(i) Occupation or economic activity/(ies) responsible for the source of income;
(j) Business and personal contact details;
(k) Capacity in which the business is being transacted, (including details of the representative relationship (if applicable));
(l) Information regarding the customer's character and integrity (for customers other than customers who are visitors to the island and not transacting business in the course of, or pursuant to a work permit situation);

[109] POCA section 120(2) & (3). POCA (MLP) Regulations, r.7(5) where customer information is defined and same includes the TRN or other relevant reference number and the identity of the settler and beneficiary in arrangements involving settlements or trusts as per regulation 13(1)(c).

(m) Any other particulars necessary to complete its KYC requirements and to assess among other things, the likelihood that the account will be used for significant transactions.

Customer Identification for Natural Persons (whether resident in the jurisdiction or not)

126. The following information[110] must be obtained from all prospective customers:

(a) Full true name and names used;

(b) Correct permanent address, including postal address (if different from the permanent address[111]);

(c) Date and place of birth;

(d) Full name, date of birth, current and previous permanent address of the joint holder of the account;

(e) Nationality;

(f) Taxpayer Registration Number (TRN)[112];

(g) Subject to paragraph 118 below), at least two (2) references (for customers other than long standing customers) and customers who are visitors to the island and not transacting business in the course of, or pursuant to a work permit situation;

(h) Contact numbers (work; home; mobile/cell;)

(i) Institutions should also require the submission of a photograph of the customer for their records. In the case of customers who are visitors to the island and not transacting business in the course of, or pursuant to a work permit situation, this

Comment [CM2]: This seems to be a requirement that should be applied where applicable and not 'as of course'.

For eg. one-off transactions being facilitated for a customer resident overseas with established banking relationship with a licensed bank in that overseas jurisdiction and whose transaction is being facilitated by the local DTI for the purposes for eg. of effecting a wire transfer; payment of a bill or invoice etc.

Comment [CM3]: This seems to be a requirement that should be applied where applicable and not 'as of course'.

For eg. one-off transactions being facilitated for a customer resident overseas with established banking relationship with a licensed bank in that overseas jurisdiction and whose transaction is being facilitated by the local DTI for the purposes for eg. of effecting a wire transfer; payment of a bill or invoice; etc.

[110] POCA (MLP) Regulations, 2007 r. 7(5) for the definition of "customer information"

[111] Note also 2008 Supreme Court (unreported) decision in the dual citizenship case of Richard Azan v. Michael Stern in which Mrs. Justice Marva McIntosh ruled that an address listed on the nomination paper as Main Street, Frankfield was incomplete. The Judge however went on to rule that the address to which a document comprising the substance of the matter was sent is sufficient once the address is the same place where the defendant could be found or communicated with. Leave has been granted to appeal the decision, not to set aside the service and to strike out a Fixed Date Claim Form, notice of presentation of election petition and security filed by Richard Azan. The Appeal was dismissed.

[112] Under the POCA (MLP) Regulations, regulation 7, customer information "includes the applicant for business's full name, current address, **taxpayer registration number** or other reference number, date and place of birth (in the case of a natural person) and, where applicable, the information referred to, at regulation 13(1)(c), TP (Reporting Entities) Regulations, (i.e. identity of beneficial owner). Under section 120 of the POCA, customer information also refers to the customer's TRN which forms a part of the information an institution must present/produce in compliance with a customer information order.

requirement can be fulfilled by provision of an official identification which ordinarily carries a photograph such as drivers licence or passport;

NB. The foregoing is required in relation to all holders of the account and beneficiaries (interim and/or ultimate).

126. Bank of Jamaica has advised the financial sector that under the POCA (MLP) Regulations, customer information includes the TRN or other reference number (in the circumstances this may include NIS or other official number issued by a Government department or unique reference numbers generated by the financial institution). However before proceeding with a transaction, 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.

127. Persons who would not reasonably be expected to have TRNs would include citizens of other countries who are:

(a) visiting the island (eg. Tourists; persons attending seminars or training workshops & courses; persons who are in the island pursuant to work permit arrangements or study arrangements (eg. students enrolled with programmes and/or educational institutions are accredited with the Ministry of Education);

(b) persons passing through Jamaica to other destinations (i.e. in transit)

128. The onus will be on the financial institution to satisfy itself that the natural person with whom business is conducted is not a citizen of Jamaica and as such, is a person in respect of which a TRN would not be required. Relying on a driver's licence from the jurisdiction of residence has its limitations to the extent that it is possible for a person to have more than one driver's licence issued by different jurisdictions. As such, a person who is a citizen of Jamaica and who should be subject to the TRN requirement could bypass the requirement by tendering a driver's licence from another jurisdiction.

There is no transition period for this requirement, as such, financial institutions must take the steps necessary to ensure compliance.

Self-Employed Persons & Sole Proprietors

129. Financial Institutions should ensure that they obtain the following information and documents or their equivalent in respect of new accounts or conduct appropriate reviews of such information and documentation when conducting significant transactions for self-employed persons and sole proprietors:-

(a) Identification and other details outlined above at paragraphs 119 and 126 above;
(b) Business Registration Certificate (where applicable);
(c) Account opening authority containing specimen signature/(s) (the authority should be clear as to whether the arrangement will include a nominee or alternate operator of the account. Where a nominee or alternate is indicated, the information at (a) above must also be obtained in respect of the nominee or alternate);
(d) A financial statement of the business (depending on the size[113] of the operations or magnitude of economic activity, these should be either audited, or financial accounts which have been prepared by a person who is duly registered as a Public Accountant in accordance with the Public Accountancy Act);
(e) Documentation listed at (f), (i) and (j) at paragraph 130 below;

Membership in a recognized representative body or association is not mandated but is desirable as such memberships usually assist with regularization and transparency of the business activities of their respective members.

Bodies Corporate[114]

130. Financial Institutions should be vigilant when dealing with corporate vehicles as they may be used as a method of maintaining anonymity. In all cases the financial institutions

[113] The Development Bank of Jamaica website reflects a table of asset size and number of persons hired and categorization of micro, medium and small businesses; the Small Business Association of Jamaica's (SBAJ's) website reflects that the SBAJ's membership comprises businesses with 1-50 persons with annual turnover not exceeding USD5million and which is not a part of a conglomerate;
[114] POC (MLP) Regulations, as amended (r. 11, 12 & 13)

should fully understand the structure of the prospective corporate client, the source of that customer's wealth, and the source of funds involved in the transaction and the beneficial owners and controllers[115]. This should be the case whether the corporate client is locally incorporated or a foreign company. Financial Institutions should also ensure that they obtain the following documents or their equivalents in respect of new accounts, or undertake appropriate reviews of such information and documentation of the intensity and frequency consistent with the customer's risk profile or when conducting significant transactions for existing bodies corporate customers:

(a) Certificate of Incorporation or certificate of registration;

(b) Articles of Incorporation;[116]

(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[117], or in the case of

(i) a company incorporated and in operation for under eighteen months, in-house financial statements;

(ii) a company which meets the criteria outlined at section 159 of the Companies Act, (company accounts which are in accordance with paragraph 5 of Section II of the 7th Schedule to the Companies Act and which have been prepared by a person who is duly registered as a Public Accountant in accordance with the Public Accountancy Act).

The financial information obtained must include confirmation on whether or not the company has issued share warrants as described in section 82 of the Companies Act.

Comment [CM4]: JBA (Compliance Committee) suggested revising the requirement generally from audited accounts to Management accounts and only require audited accounts (over an agreed threshold). The suggestion was not acted on, as all companies are required to prepare audited financial statements under the Companies Act subject to the exception permitted at section 159 of the Companies Act re: companies which meet the statutory definition of 'small companies'. Management accounts could probably be accepted in respect of any financial year where in respect of the immediately preceding financial year, the FI has the company's audited accounts, and in respect of the current financial year, the audited statements would not be due. However my understanding of Management accounts vs. financial accounts is that the former is usually prepared for internal purposes; and is not subject to the GAAP; whereas financial accounts are prepared for external users, is subject to the GAAP, and must generate accurate and timely data.

[115] See POC (MLP) Regulations, 2007 (r. 11, 12 & 13); Basel Committee on Banking Supervision – Sound management of risks related to money laundering and financing of terrorism, January 2014.

[116] Under the Companies Act, 2004 (operational 2005) the requirement for Memorandum of Association has been discontinued, however, Memorandum and Articles of Association would still be relevant for the purpose of these Guidance Notes until these documentation have been updated pursuant to the new Companies Act.

[117] JBA (Compliance Committee) suggested revising the requirement generally from audited accounts to Management accounts and only require audited accounts (over an agreed threshold). The suggestion was not acted on, as all companies are required to prepare audited financial statements under the Companies Act subject to the exception permitted at section 159 of the Companies Act re: companies which meet the statutory definition of 'small companies'.

(f) A description of the customer's principal line of business and major suppliers or major customers/main target market (where applicable) (and other services or activities that materially contribute to the entity's income); and whether the entity is designated as or associated or affiliated with any charitable establishments (locally or overseas);

(g) A list of names, addresses and nationalities of principal owners, directors, beneficiaries and management officers; Evidence of the identity of the natural persons, that is to say, the individuals that ultimately own or control the company or body corporate (i.e. holding 10% or more of the voting rights[118]) must also be provided or be readily accessible directly by the financial institution at will or immediately, on request.

Verification of the information provided on the directors, who are the persons responsible for the mind and management of the body corporate with whom the relationship will be established or transaction conducted, should also be independently verified from National company registries, and other places where the information may have to be provided such as a recognized Stock Exchange[119]. Disclosures on the particulars of owners, and directors must include disclosures in relation to nominee shareholders and nominee directors and shadow directors[120].

Where the directors and beneficial owners are themselves body corporates or trustees or settlors, the obligation to identify the ultimate beneficial owner is not satisfied until the identity of the natural beneficial owner or the senior manager with responsibility for the legal person or arrangement, is ascertained;[121]

Comment [CM5]: In relation to the verification of the identity of owners, JBA Compliance Committee recommended a threshold requirement at which the verification should be applied. This would be in keeping with best practices and international practice but the POCA does not currently allow for such an approach to be taken. The POCA currently mandates obtaining identification information for ultimate beneficial owners (and incorporates a 10% ownership threshold which is applicable to companies not registered on the stock exchange) and verifying same. The item has been flagged for communication to the Ministry/NAMLC etc. for action. If the recommendation to amend the POCA is accepted then Industry recommendation of application of a general threshold for verification of shareholder ID can be acted on and requirement for Director identification for businesses that are listed on a recognized stock exchange can be simplified.

[118] POC (MLP) Regulations, regulation 13(1)(c)(iii)(A); TP (Reporting Entities) Regulations, regulation13(1)(c)(iii)(A).
[119] POC (MLP) Regulations, regulation 13(1)(c)(iii); OECD – Supervision and Enforcement in Corporate Governance, 2013.
[120] The term "shadow director" is defined in the Companies Act, 2004 (operational date 2005)
[121] POC(MLP) Regulations regulation 13(1)(c)(i)A; TP (Reporting Entities) Regulations regulation 13(1)(c)(i)A; and POC (MLP) Regulations, regulation 13(1)(c)(ii)(B).

Disclosures on the particulars of owners, and directors must include disclosures in relation to nominee shareholders, nominee directors (provided these nominations are in relation to corporate holdings within the meaning of the Companies Act) and shadow directors.

(h) Group/Corporate structure, where applicable;

(i) A copy of the licence/approval to operate where the principal line of business is one that falls under a regulatory/supervisory body or is a regulated activity (i.e. a licence; or other authorization must be obtained in order for the business activity to be legitimately undertaken);

(j) Tax Compliance Certificate (TCC)[122] or other equivalent official confirmation from the relevant tax authorities of compliance with income tax obligations;

(k) The source of wealth of the corporate customer and the source of funds being placed with the financial institution.

Membership in a recognized representative body or association is not mandated but is desirable as such memberships usually assist with regularization and transparency of the business activities of their respective members.

131. KYC details for body corporates that must be in place for basic KYC requirements and in the event that the financial institution is served with a customer information order, it is the same information above at paragraph 125 on natural customers.

132. KYC due diligence for corporate customers may[123] be satisfied if the corporate customer has established to the financial institution's satisfaction that it is a company listed on the

[122] TCCs (or equivalent confirmation of tax compliance) valid for one year can be obtained provided the taxpayer's information in the database of the Tax Administration Jamaica can support the issuing of a TCC/or other such confirmation for that period. The application process involves submission of the application form + requisite clearance letters as outlined on the TAJ's website. Electronic/online applications can also be facilitated. Applications can indicate whether or not the TCC/or other such confirmation is for several purposes (i.e. single purpose (eg. accessing banking facilities) or multipurpose (accessing banking facilities; importation of goods etc.). Once the purpose of the TCC/or other such confirmation changes, the likelihood of achieving eligibility for a TCC/or other such confirmation that is valid for one year decreases because there would be no supporting information in the TAJ's database in relation to the new purpose for the TCC/or other such confirmation that is indicated by the Taxpayer.

Jamaica Stock Exchange's public listing of companies and is in good standing with that body.

(a) Good standing confirmations include ensuring the JSE or other stock exchange explicitly confirms-

(i) That the filing of audited financial statements are prompt and up to date;

(ii) That there are no pending disciplinary actions against the company;

(iii) 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)

(b) Companies listed on more than one exchange should be in a position to provide the above confirmations from the respective exchanges on which the company is listed.

(c) This method of conducting KYC 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.

133. Where the corporate customer is a part of a group of companies, the financial institution should ensure that it is fully aware of the ultimate beneficial owners/controllers of the company and that it is aware of any group arrangements or affiliates that could present a reputational risk to the financial institution. When there is doubt concerning the identity of a company, its controllers, directors, shareholders or ultimate beneficial owners/shareholders, a search should be conducted at the Registrar of Companies or equivalent authority for registration or the requisite trade or professional regulatory body or other appropriate source.

Comment [CM6]: Should this requirement be retained; or is it sufficient if the FI is satisfied that the records of the stock exchange are:-

- current; and
- contain the details required for bodies corporate and their directors and shareholders?

[123] POC(MLP) Regulations, regulation 13(3) reflects that the exemption identification procedures approach outlined in relation to a body corporate, a director or shareholder are not applicable in any case involving a suspicion of money laundering. See also TP (Reporting Entities) Regulations 13(1)(c) - closing paragraph.

Partnerships[124]

134. Financial institutions should fully understand the obligations and responsibilities and entitlements arising under the partnership, the source of wealth accumulated by the Partnership, the source of funds involved in the transaction and the controllers and beneficiaries thereunder (where this differs from the persons indicated as the Partners). This should be the case whether the partnership is locally established or established outside of Jamaica. Financial Institutions should also ensure that they obtain the following information and documents or their equivalents in respect of new accounts or undertake appropriate reviews of such information and documentation when conducting significant transactions involving partnerships or similar arrangements (by whatever name called):-

(a) Partnership Deed (or other Instrument in writing which is duly signed by the Partners and which confirms the fact of the establishment of the Partnership);

(b) Business registration certificate (where applicable) or equivalent instrument as the case maybe;

(c) The information regarding the authority to undertake or agree to engage in transactions which legally bind the partnership; signing authority for the account mandate and specimen signatures;

(d) A financial statement of the business which should either be:-

(i) Audited, in the case of partnerships in operation for over 18 months and whose operations, if it were a company, would be in excess of the operating levels of a company described at section 159 of the Companies Act; or

[124]New legislation (General Partnership Act, Limited Partnership Act, Limited Liability Partnership Act, etc.) is currently being drafted which will impact the definition and operation of partnerships in the future. This new legislation allows for partnerships to have separate legal standing and therefore would have separate liability from its partners. The first part of the legislation was presented to parliament in early 2016 for their consideration.

(ii) In the case of partnerships in operation for over 18 months and whose operations, if it were a company, would either meet or fall below the operating levels of a company described at section 159 of the Companies Act, business accounts prepared in accordance with paragraph 5 of Section II of the 7th Schedule to the Companies Act, and which have been prepared by a person who is duly registered as a Public Accountant in accordance with the Public Accountancy Act;

(e) A description of the principal line of business;

(f) CDD for Partners, management officers and beneficiaries under the partnership (where these differ from the partners); nationalities and evidence of the identity of the partners, must also be provided or be readily accessible directly by the financial institution at will, or immediately, on request.

(g) Details of entities, (incorporated or unincorporated) with which any one or more of the partners is affiliated. For the purpose of this requirement, details include name, business or registered address of the affiliated entity and the nature of the relationship with the affiliated entity;

(h) Tax Compliance Certificate or other equivalent official confirmation from the relevant tax authorities of compliance with income tax obligations;

(i) Confirmation of the source of funds being placed with the financial institution and source of wealth of the partnership.

Principals and Beneficial Owners under, Trusts, Settlements and Other Legal Arrangements[125]

135. Financial Institutions should ensure that they obtain the following information and documents or their equivalents in respect of new accounts or conduct appropriate reviews of such information and documentation when conducting significant transactions involving trusts, settlements and other legal arrangements:-

(a) Trust Deed or Instrument under which the trust, settlement or other legal arrangement, is derived[126] and evidence of the registration of the deed or other instrument. Appointments as Trustees that occur pursuant to section 10 of the Trusts Act are subject to the additional requirements that trusts relating to land should be registered with the Registrar of Titles, and otherwise, registration should occur with the Island Record Office[127];

(b) Identification and other details outlined above at paragraphs 119 and 126 are equally applicable in relation to all principals of trusts, settlements and other legal arrangements and beneficial owners thereof who are natural persons. Where such principals and beneficial owners are themselves body corporates or trustees or settlors, then the obligation to identify the ultimate beneficial owner is not satisfied until the identity of the natural beneficial owner is ascertained[128]. Verification of identification information provided on such principals and beneficial owners should be independently verified from for example national registries (which record information on trusts and/or other legal arrangements, where these exist). Otherwise ownership and director identification details should, at a minimum be accessible from the senior manager with responsibility for the trust or other legal arrangement[129].

[125] POCA (MLP) Regulations, 2007 (r. 11, 12 & 13) as amended.
[126] Trusts Act; Trustees, Attorneys and Executors (Accounts and General) Act - These statutes govern the activities of Trustees.
[127] Trustee Act, section 10(6)
[128] POC(MLP) Regulations amended 2013 regulation 13(1)(c)(i)A; TP (Reporting Entities) Regulations, regulation 13(1)(c)(i)A.
[129] POC (MLP) Regulations, regulation 13(1)(c)(ii)(B)

(b) List of names, addresses and nationalities of principal trustees or directors or other persons who are members of the board (or other body by whatever name called) of the trust, settlement or other legal arrangement that is responsible for the governance and oversight of the trust, settlement or other legal arrangement; beneficiaries and management officers. Where such principals and beneficial owners of the board members (or other body by whatever name called) are themselves body corporates or trustees or settlors, evidence of the identity of the natural persons, that is to say, the individuals that ultimately own or control those members must also be provided or be readily accessible directly by the financial institution at will or immediately, on request[130]. In relation to the directors of trusts, settlements or other legal arrangements, as these persons would be responsible for the management of such trusts, settlements or other arrangements with whom the relationship will be established or the transaction conducted, the verification of the information provided on the members of the board or other body (by whatever name called) should also be independently verified from National registries, and other places where the information may have to be provided[131]. The foregoing disclosures must also include disclosures in relation to nominee shareholders and nominee directors.

Charities

136. Special care should be taken by financial institutions in dealing with unincorporated bodies (such as foundations; trusts etc.)[132]. The legal relationship should only be established with the principal officers or principal representatives of the body, and information on these persons, the purpose of the account and intended nature of the business relationship must be obtained.

[130] In relation to verification of the identity of Owners see comment on paragraph 130(g).
[131] POC (MLP) Regulations, regulation 13(1)(c)(iii); OECD – Supervision and Enforcement in Corporate Governance, 2013.
[132] FATF's 2003/4 AML and CFT typologies exercise covering, inter alia, non-profit organizations. (See also FATF Best Practices – Combating the Abuse of Non-Profit Organisations, June 2013 & FATF Best Practices – Transparency and Beneficial Ownership, October 2014)

137. Financial Institutions should therefore ensure that they obtain the following information and documents or their equivalents in respect of new accounts or significant transactions involving charities, or non-profit organizations (NPO):-

(a) In the case of a charity which is established as a body corporate by incorporation as a company or otherwise, the articles of incorporation[133] and certificate of incorporation or charter, statute or other like instrument by which it is established;

(b) The constitution (as defined under the Charities Act) of the charity or NPO;

(c) Evidence of registration in accordance with the Charities Act, 2013;

(d) In relation to charities or NPOs which have been established as bodies corporate, whether as companies or otherwise, the information set out at paragraph 125 (c), (d) and (e) of these Guidance Notes;

(e) List of names, addresses and nationalities of principal owners or of the beneficial owners (if different from the principal owners)(i.e. to say the individuals who ultimately own or control the charity or NPO), directors, trustees, settlors or other persons who are governing board members as defined in the Charities Act, and management officers;

(f) A financial statement of the charity or NPO which should prepared as outlined in the Charities Act or Regulations thereunder and which should be:-

(i) Audited, in the case of charities in operation for over 18 months and whose operations, if it were a company, would be in excess of the operating levels of a company described at section 159 of the Companies Act; or

(ii) In the case of charities in operation for over 18 months and whose operations, if it were a company, would either meet or fall below the operating levels of a company described at section 159 of the Companies Act, business accounts prepared in accordance with paragraph 5 of Section II of the 7th Schedule to the Companies Act, and which have been prepared by a person who is duly registered as a Public Accountant in accordance with the Public Accountancy Act;

[133] Refer to paragraph 130, on Bodies Corporate, for a definition.

(g) A list of the charity's significant donors and recipients of financial and other assistance (including name, address, nationality; main business activity or occupation and where the donor is a body corporate, trust, settlement or other legal arrangement, the names of the natural persons who are the directors and beneficiaries thereof). Financial institutions will need to ascertain whether the information provided by the charity, is sufficient to allow for a determination to be made by the financial institution regarding the risks of doing business with that charity including the risk of a terrorist financing activity being facilitated through dealings with that charity and the extent of business that is facilitated with or involving that charity;

(h) Evidence of the due diligence done to confirm the bona fides of the source of funds received from the donor and source of wealth of the donor.

CUSTOMERS RESIDENT OVERSEAS

138. In addition to the foregoing considerations additional factors must be included in the due diligence and broader KYC processes and measures that are applied.

139. Financial institutions are required to ensure that, among other things, a financial institution's AML/CFT measures include paying special attention to all business relationships and transactions with any customer resident or domiciled in a territory specified in a list of applicable territories published by notice in the Gazette by a supervisory authority.[134] For the purposes of these Guidance Notes, the jurisdictions that would ordinarily be targeted for this special attention include jurisdictions flagged by:-

(a) FATF;
(b) One or more of the other 8 FATF Styled Regional Bodies ("FSRB");
(c) UNSEC, and
(d) A country with which Jamaica is Party to a treaty that requires a Party to such treaty to take certain actions in relation to nationals of either Party in accordance with the circumstances outlined in such treaty.

[134] POCA (Amendment) Act, 2013 section 94(4)(b).

(Refer to Section III above at paragraph 64 above on "*Advisories and Publications issued in relation to certain Jurisdictions*")

140. Financial institutions should exercise a high level of caution when establishing business relationships with foreign companies that have nominee shareholders or bearer shares. If the ultimate beneficiary/ies or beneficial shareholders/s cannot be reliably established or there are no reliable measures in place to monitor any changes in the ownership structure or to capture details of the holder of bearer shares, then the relationship should **not** be commenced, or where a business relationship has already been established, this relationship should be legally terminated.

141. Institutions should also exercise particular care when dealing with overseas counter-parties or financial institutions acting for overseas clients, where to the local financial institution's knowledge, the overseas counter-party or representative financial institution is not subject to AML/CFT laws and regulatory arrangements at least as stringent as those applicable to Jamaica. In this regard the guidance on Introduced Business and Professional Intermediaries etc. is particularly relevant. Additionally, financial institutions should carefully scrutinize any transaction proposed to be carried out with any client, counter-party or financial institution situated in a jurisdiction with weak or non-existent AML/CFT/ Non-proliferation of weapons of mass destruction programmes or with a known history of involvement in drug production, drug trafficking, corruption, money laundering or terrorist financing or renowned for industry sensitive activities such as the production and transportation of arms; or whose citizens or which is itself the subject of targeted financial sanctions as indicated in these Guidance Notes. Financial institutions should also seek to keep abreast of steps being taken by such jurisdictions to effectively deal with such matters.

NATURAL PERSONS RESIDENT OVERSEAS

142. The identification, and KYC requirements for natural persons resident in Jamaica also apply to natural person's resident outside of Jamaica. Financial Institutions are required to obtain the

same identification documentation or their equivalent for prospective customers resident outside of Jamaica. Deposit taking financial institutions should also ascertain why a non-resident client has chosen to open an account in the local jurisdiction[135].

OVERSEAS BASED BODIES CORPORATE

143. The requirements for the KYC and customer due diligence for domestic corporate customers are also applicable to overseas corporate bodies with which a financial institution does business. Comparable documents to those listed in paragraph 130 should be obtained, when opening accounts for companies or any bodies corporate incorporated outside of Jamaica.

144. The financial institution would be expected to ensure that the foregoing is considered in the context of a jurisdiction which is not a jurisdiction that has been subject to any one or more of the following actions:-

(a) identification by the FATF; CFATF or any FRSB as a jurisdiction with strategic deficiencies or weaknesses in its AML/CFT/ Combating the proliferation of weapons of mass destruction framework;

(b) identification by the United Nations as a jurisdiction subject to targeted financial sanctions pursuant to UN Resolutions on Terrorism and Terrorist Finance – i.e. UN Resolutions 1267 (1999), 1373 (2001), and related resolutions; and targeted financial sanctions pursuant to UN Resolutions on the proliferation of weapons of mass destruction – i.e. UN Resolutions 1718 (2006), 1737(2006), 1747(2007)1803(2008), 1874(2009) and 1929(2010); or

(c) identification as an 'applicable territory' by a supervisory authority pursuant to section 94(4)(b) of POCA by notice published in the Gazette.

[135] POC (MLP) Regulations and the TP (Reporting Entities) Regulations include in the description of 'high risk' customers, 'a person who is not ordinarily resident in Jamaica.

145. Particular attention should be paid to the place of origin of identity and other documents provided in such circumstances, and the background against which they are produced, bearing in mind that standards of control vary between countries. A financial institution may have to request certified copies of documents notarised by a foreign official such as a notary public, or county clerk in addition to making appropriate enquiries with overseas authorities, statutory organizations, overseas credit reference agencies, or similar bodies.

Transaction Counter-parties

146. A counterparty to any transaction with a financial institution should be subject to the same due diligence undertaken in relation to customers as far as this is applicable in the circumstances.

VERIFICATION OF CDD, KYC & TRANSACTION DETAILS

147. The name, permanent address and employment/business details of a customer should be verified by an independent source, (i.e. by a source other than those provided by the customer), as per the following examples:

(a) Requesting sight of a current utility bill for the customer's place of residence (for example, electricity, telephone, and water) or cable receipt in the name of the customer[136]; requesting sight of correspondence from an independent source such as a central or local government department or statutory body. Documents addressed to, for eg. P.O. Box numbers may be relied on where there is no street number or other coded identification to identify the physical location of the address or where the P.O. Box number comprises a routine part of the standard mailing address and it is confirmed that the customer receives mail using that mailing address.

(b) Checking a local telephone directory and calling the number for verification purposes;

[136] POC (MLP) Regulations, regulation 7(5) definition of 'satisfactory evidence'

(c) Checking the Voters' List [137];

(d) Spot check visits to the home address or work place (where practical i.e. where the home or work place of the customer is in relatively close proximity to any locations where the financial institution is represented or has a physical presence);

(e) Independent confirmation of national identifications with the relevant Government Authorities, eg. (confirming drivers licences with the records of the Collectorate; confirming Voters ID with the relevant electoral office of Jamaica confirming Passports with the Passport, Immigration and Citizen Agency and confirming employee identification cards with the indicated employers. Particularly if the document appears to be tampered with or there is doubt about the accuracy of any information contained in the Identification;

(f) Confirming customer's details and status of employment independently with the employer; confirming customer's salary scale by obtaining general information from the employer of the salary scale and benefits applicable to the level indicated by the customer;

(g) Cross-checking KYC details with other financial institutions or businesses that the customer indicates financial business is transacted with (for instance the issuing bank in the case of cheque transactions; the insurance company from which the funds are indicated as being obtained, the cambio from which the foreign currency was received, or the remittance company through whom the funds were sent). In so doing financial institutions will need to be guided by the respective Agreements with the customer which should ideally reflect that the customer's consent has been obtained to do this type of check. (See also paragraph 148 below)

(h) Cross-checking KYC details for one account holder with the other holder of the account and vice-versa (however if this check is done it should not comprise the only effort at establishing independent verification of information provided by an account holder).

[137] Checking with the Post Office which has listings according to constituency or purchasing the CD Rom from the Electoral Office of Jamaica. The latter option is only useful if the institution is in possession of the customer's voter identification number as this number is needed to access the customer's details from the CD ROM. The information cannot be accessed otherwise from the Electoral Office of Jamaica.

(i) Cross-checking KYC details provided with other affiliated companies within the corporate group with whom the customer has also done business. (In so doing financial institutions will need to be guided by the respective Agreements with the customer which should ideally reflect that the customer's consent has been obtained do this type of check.)

(NB. Reference to the customer also includes reference to the Applicant for business)

Verification of Identification Details Post Commencement of Business Relationship

148. POCA (MLP) Regulations, 2007 (and as amended 2013) (r. 7) speaks to situations in which satisfactory evidence of a customer's identification can be obtained as soon as is reasonably practicable after contact is first made between that person and an applicant for business. Before proceeding in this manner, a financial institution must be in a position to provide documentary evidence of the evaluation it undertook to satisfy itself that it could proceed with the transaction. This includes evidence of considerations which at a minimum should include-

(a) The nature of the proposed business relationship;
(b) The nature of the transaction/(s) contemplated;
(c) The geographical location of the parties;
(d) Practicality of proceeding viz. entering into commitments; or facilitating transactions before confirmation of the identification is obtained, (included in this consideration is whether proceeding is essential to not interrupting the normal conduct of business);
(e) Assessment of the risks to the institution if it proceeds without confirmation of the customer's identification.

Confirmation of KYC/ or CDD with the assistance of other financial institutions

149. In some cases, a financial institution may require the customer to issue instructions to another financial institution with whom he/she/it has dealings and which institution is

able to provide appropriate KYC verification for the customer in question. A financial institution may therefore need to approach another on a non-competitive basis, specifically for the purpose of verifying certain KYC/ CDD details. Where this is the case, it is expected that members of the industry will formulate industry agreements and/or protocols on these matters, within the specific constraints of the law. Where KYC/ or CDD verification is pursued through this option and the information is still not forthcoming from the institution from whom the assistance is requested, then unless the information is obtained,

(a) the transaction should not proceed; or

(b) where commenced in circumstances where it was deemed reasonable to proceed ahead of the verification, should not be completed; or

(c) where the relationship is already formed (eg. an account is opened ahead of verification) then no other service or facility or transaction should be provided or conducted with, on behalf of, or in relation to this customer;

unless and until the appropriate KYC/ or CDD verification information has been received whether from the institution from which the information was requested or from an alternative but equally reliable independent source. The financial institution must ensure that it is legally in a position to terminate the account/transaction or sever the business relationship where the verification of KYC/ or CDD details cannot be obtained.

In order to facilitate compliance with the law it is critical that institutions respond in a timely manner to each other's requests for assistance with the verification of KYC/ or CDD information.

Transaction Verification

150. Transaction verification involves ensuring that the transaction indicated and conducted is the one intended by the customer/counterparty. Verification processes therefore contemplated by these Guidance Notes include -

(a) Ensuring that agents acting on behalf of customers/counterparties have tendered evidence of the requisite authority and that the instructions pertaining to the transaction at hand are verified. Eg. Conducting a $500,000 transaction when the intention or authority was for a $50,000.00 transaction.

(b) That transactions indicated are in essence the transactions conducted and are genuine in terms of correct documentation; proper invoicing; source of asset ownership, source of funds etc.

(c) Consistency of transaction being conducted with transaction patterns for the industry/sector/business or the account history.

(d) Commercial reality or method by which the transaction is conducted should be consistent with approved or accepted industry practice or should clearly serve and reflect economic and/or lawful purpose. Eg. Transactions in which the payment is not directly reflected between the entity and the counterparty, should be flagged.

149. Verification procedures would therefore include-

(a) Ensuring that the customer or counterparty to the transaction is not a listed entity under the TPA; or a person who is personally subject to criminal designation eg. Drug kingpin; or is not operating from a jurisdiction that is the subject of a public statement reflecting it has weak or non-existent AML/CFT laws and measures.

(b) Establishing the source of funds or source/origin of the property that is the subject of the transaction.

(c) Checks (where applicable) with the relevant Trade/Service regulator to ensure the customer or counterparty is not subject to regulatory sanctions that would make it illegal or unlawful for the transaction at hand to be undertaken.

(d) Measures employed to satisfy the financial institution that any applicable industry requirements or laws are not being breached or the breach thereof is not facilitated by the transaction being conducted or to be conducted with the financial institution.

(e) Measures employed to satisfy the financial institution that agents acting on behalf of customers or counterparties have tendered evidence of the requisite authority and that the instructions pertaining to the transaction at hand are verified.

150. Under the POC (MLP) Regulations, a record of each transaction conducted must be kept in a manner that will facilitate the reconstruction of such transactions[138]. A financial institution should also ensure that evidence of transaction verification it has undertaken is documented and retained either with the transaction itself or in a manner which allows for ready or immediate recollection on request or as necessary, and readily available to the designated authority, competent authority. This information should also be readily available to the auditors of the financial institution.

RELAXED AND ENHANCED IDENTIFICATION AND KYC REQUIREMENTS

151. The revised FATF Recommendations allow for either enhanced measures or simplified measures to be applied for specifically defined customers and products which have been assessed as presenting a higher risk or lower risk of money laundering or terrorist financing[139]. Where higher risks for ML or TF are identified by a country, that country should either prescribe that financial institutions and DNFBPs take enhanced measures to manage and mitigate these higher risks or require these persons to ensure that such information is taken into account when undertaking their respective risk assessments[140].

[138] Regulation 14(4)
[139] FATF Guidance Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion, February 2013- Paragraph 68
[140] Revised FATF Recommendations – Paragraph A4 - Interpretive Note to R1

Meeting this requirement, among other things, involves:-

a) Conducting an assessment as discussed above Section IV of these Guidance Notes. The assessment methodology (including data source; active periods covered by the assessment; basis for methodology and findings) should be documented and readily available to the Supervisor, designated authority and/or external auditors;

b) Ensuring the assessment is reflective of the country's assessment of its ML and TF risks;

Comment [CM7]: The requirement for consistency was deliberately not proposed because it is felt that the requirement for consistency could be confusing particularly where, based on the FI's own assessment, the factor assessed should be placed in a risk rating which is higher or lower than that assessed by the country.

c) Ensuring the assessment is kept up to date (i.e. assessments being undertaken periodically (at least once per quarter or more frequently where warranted);

d) Having the Supervisor review the ML and TF risk profiles and risk assessments that have been prepared by the financial institution to monitor whether the financial institution's operations are consistent with the risk assessments and risk profiles that it has generated.

Relaxed Requirements

De Minimis Transactions

152. Exemptions from the requirement for identification procedures are applicable in the case of de minimis transactions. Under the POC (MLP) Regulations, regulation 8, the identification procedures outlined in regulation 7 are not applicable to transactions amounting to or less than US$250.00 or the equivalent in any other currency. The limit can be varied by the Minister by order published in the Gazette and the variation can be addressed by prescribing different amounts in respect of different categories of business[141]. Regulation 7 requires the following to be in place-

(a) Satisfactory evidence of the customer's identity;

(b) Verification procedures to confirm the customer's identity;

[141] The POC (MLP) Regulations, amended 2013 regulation 8(1)(b).

(c) Updates to KYC information at least every seven (7) years or more frequently as warranted by the risk profile of the business relationship;

(d) Termination of the business relationship or not proceeding with the business relationship if the customer's identification cannot be verified; or if purpose and nature of the business relationship cannot be verified.

153. There is however no exemption from extending risk assessments to transactions of this nature. According to the FATF simplified measures are permissible where a lower risk has been identified and this is consistent with the country's assessment of its ML and TF risks[142]. Initially, the inclusion of the concept of a de minimis level in the AML framework, was based on the observations of the financial crimes investigative authorities that the transactions which appeared to present risks of a financial crime being conducted and which featured significantly in the STRs generated, were those which reflected amounts in excess of approximately USD$250. It should be noted that the AML/CFT laws do not reflect that the de minimis approach absolves financial institutions from conducting their own risk assessments in relation to such transactions.

154. For de minimis transactions procedures for identification and transaction verification need not be invoked, however all other AML/CFT precautions and requirements, remain applicable. This therefore means that for the purposes of record keeping, financial institutions should ensure that the following measures are taken:

(a) Transaction records should reflect salient details, including:

(i) The customer's name;
(ii) The customer's permanent address and jurisdiction of residence or incorporation/ establishment;
(iii) Transaction type;
(iv) Transaction amount;
(v) Transaction currency (and Jamaican dollar equivalent if the transaction is in foreign currency); and
(vi) Identification type and number;

[142] FATF Recommendations 2012– paragraph A5 - Interpretive Note to R1

(vii) TRN (where applicable) or other reference number.

(b) Transactions are Monitored/Reviewed to detect /prevent Layering/Structuring – (i.e. transactions by the same person (connected transactions) or transactions conducted separately but which are intended to take effect as one transaction for the benefit of one person. Connected transactions which take place on the same day which each meet the de minimis limit but which altogether exceed the de minimis limit, should be reviewed to determine whether procedures for identification and transaction verification should be applied notwithstanding the transaction amount, since such transactions could constitute layering or structuring to avoid KYC/CDD requirements.

Transactions for which the de minis approach does not apply

155. Transactions subject to Required Disclosure (Suspicious Transactions) - The de minimis exemption is not applicable to transactions that require disclosure under sections 94 and 95 of the POCA, (r.8(1)) or disclosure under sections 16 or 17 of the TPA (r.8(1)).

156. Remittance Transactions - The de minimis approach is not applicable to remittance transactions (r. 8(2) of the POC (MLP) Regulations and (r. 8(2) of the TP (Reporting Entities) Regulations).

Transactions to which the de minis approach should not apply

157. Critical Transactions - The Bank of Jamaica considers the following to be critical transactions for the purposes of these Guidance Notes-

(a) Transactions effectively amounting to the opening of accounts and/or closing of accounts;

(b) Transactions that are assessed as 'high risk' or which are described in the AML/CFT laws as falling in the category of 'high risk'.

Accordingly it is expected that transactions which in dollar value equate to the de minimis limit but which in nature are "critical transactions**"** should be subject to the usual KYC and CDD policies and procedures.

ENHANCED REQUIRMENTS

158. Heightened requirements are applicable where either the risk of doing business, or establishing or maintaining certain relationships with certain customers or counterparties increases. Such circumstances of increased risk arise for instance by virtue of the positions held or functions undertaken by the customer or transacting counterparty, or in relation to customers or transacting counterparties in respect of which the financial institution conducting business will either not have, or will have very limited opportunity to transact business directly with that customer or counterparty on a face-to-face basis and as such will have to rely on the judgment and information provided by a third Party.

159. Risks also increase if the customer or counterparty resides in, or operates from, a jurisdiction which is the subject of an adverse rating or an international sanction related to identified deficiencies in that jurisdiction's prudential, regulatory or AML/CFT// Combating the proliferation of weapons of mass destruction framework. Risks also increase if the customer or counterparty resides in, or operates from, a jurisdiction which is subject to a regulatory or supervisory framework that is incompatible with the supervisory or regulatory framework in Jamaica. Incompatibility would be measured by the absence or presence of any one or more of the following circumstances such as:-

(a) The financial activity not being subject to any regulation or supervision, or is not subject to an equivalent regulatory or supervisory framework;

(b) The person undertaking an intermediary, agent or representative role in relation to the transacting counterparty or customer is not subject to AML/CFT laws and regime; and

(c) The existence of secrecy laws and other legislative or policy requirements that adversely impact or hinder or prevent effective regulatory collaboration or cooperation from taking place between BOJ and the regulatory/supervisory authorities in that jurisdiction.

160. Accordingly, under POC (MLP) Regulations and TP (Reporting Entities) Regulations, relationships or transactions that are identified as high-risk include –

(a) PEPs,

(b) A person who is not ordinarily resident in Jamaica;

(c) A person acting as a trustee for another in relation to the business relationship or one-off transaction concerned;

(d) A company having nominee shareholders or shares in bearer form; or

(e) Such other class or category of persons specified by the supervisory authority by notice published in the gazette.

The list of relationships or transactions reflected in the regulations is not exhaustive and can be expanded by the supervisory authority under the POCA, by notice published in the gazette. As such, **financial institutions are subject to the statutory mandate to establish a risk profile regarding all respective business relationships and one-off transactions**[143]. The law defines "risk profile" as a formal assessment made by the regulated business concerned as to the level of ML risk posed to the regulated business by the business relationship or transaction concerned.

161. Additional circumstances which, based on the foregoing, appear to increase the risks to a financial institution doing business include:-

(a) Verification of identification post commencement of the business relationship;

(b) Introduced business;

(c) Trust or Settlor Accounts;

(d) Accounts opened by Professional Intermediaries;

(e) Private banking clients; Transferring clients; Non-face-to-face customers; Transactions via emerging technology; correspondent banking; payable through accounts; Countries with inadequate AML/CFT/ Combating the proliferation of weapons of mass destruction

[143] The POC(MLP) Regulations amended 2013 –-regulation 7A; The TP (Reporting Entities) Regulations amended 2013 – regulation 6A

frameworks; Transactions undertaken for occasional customers; Custody arrangements; Wire transfers and other electronic funds transfer activities.

INTRODUCED BUSINESS[144]

162. In circumstances where business is being introduced, the ultimate responsibility is on the recipient financial institutions to know the referred customer and his/her/its business and to establish the adequacy of the KYC/ CDD details regarding this business being introduced. Financial institutions may consider themselves entitled to rely on the identification procedures that the introducers have performed if the circumstances outlined in regulation 12(1)[145] and 12(1A) of the POC (MLP) Regulations are in place. At a minimum, establishing that the circumstances of 12(1) and 12(1A) have been met, requires that financial institutions must, among other things:-

(a) carefully consider the fitness and propriety of introducers and assess the adequacy of the customer identification and due diligence standards that the introducers maintain, and to which they are held, pursuant to the AML/CFT laws and framework which govern the introducer;

(b) be satisfied that introducers adhere to minimum "Know Your Customer" and " Customer Due Diligence" standards as identified within these Guidance Notes;

(c) be satisfied that, based on the risk profile[146] the customer or transaction is not high risk;

(d) be able to verify the due diligence procedures undertaken by the introducer at any stage and the reliability of the systems put in place to verify the identity, financial history and KYC details of the customer;

(e) be able to procure and review all the relevant identification data and other documentation pertaining to the customer's identification, financial history and other KYC data, either as soon as is reasonably practicable after the introduction or without delay on the request of the financial institution.

[144] POC (MLP) Regulations 7, and 12; TP (Reporting Entities) Regulations 5 and 12; FATF Recommendation 17
[145] TP (Reporting Entities) Regulations regulation 12(1)
[146] POC (MLP) Regulations, regulation 7A; See the TP (Reporting Entities) Regulations, regulation 6A;

(f) A financial institution's compliance with this requirement will be assessed by the Supervisor based on the availability of the CDD & KYC information for review by the Supervisory Authority;

163. Whenever possible, the prospective customer should be interviewed; and where it has been determined that the information provided in relation to the customer is not adequate or the mechanism by which the information was obtained is deficient, then the financial institution must conduct its own KYC/CDD.

164. The information provided to the financial institutions must also be available to the Supervisory Authority as well as to the Competent Authority and Designated Authority under the POCA[147].

TRUST ACCOUNTS

165. Subject to paragraph 166 below, where an account is being opened by a trustee/settlor pursuant to trust arrangements, the identity of **all** parties and beneficiaries and ultimate beneficiaries to the transaction must be ascertained and recorded in keeping with the AML and CFT Regulations[148]. This would also include identification of the trustees, settlors and grantors, the beneficiaries and ultimate beneficiaries of the trust account, source of wealth from which the proceeds of the trust are derived, as well as the source of funds involved in the transaction, and the purpose and details (i.e. terms) of the trust arrangement for the trust or settlement.

ACCOUNTS OPENED BY PROFESSIONAL NTERMEDIARIES[149]

166. Professional intermediaries generally include pension funds, collective investment schemes and other fund managers, as well as lawyers (see related guidance at paragraph

[147] POC (MLP) Regulations 2007 and amended 2013, regulation 14(21)(2) and (4).
[148] POC (MLP) Regulations, (r. 11, 12 & 13);-TP (Reporting Entities) Regulations (r. 11, 12 & 13)
[149] POC (MLP) Regulations (r. 11, 12 & 13); TP (Reporting Entities) Regulations (r. 11, 12 & 13); FATF Recommendation 17

168 below), securities dealers and stock brokers managing single or pooled accounts held on deposit or in escrow for clients.

A financial institution may consider itself entitled to rely on the professional intermediary's customer identification due diligence process but only where there is compliance with the POC (MLP) Regulations and TP (Reporting Entities) Regulations, (which are equally applicable to introducers and professional intermediaries).

167. Financial Institutions should note that, notwithstanding the ability to place reliance on third Party introductions, the statutory obligations under the law for identification of the customer and beneficial owners, is placed on the financial institution. Accordingly, the financial institution must ensure its procedures, policies and measures on CDD and KYC including those established to facilitate reliance on third Party identification processes, are compliant with the AML/CFT laws and framework[150] and allow for its undertaking the requisite KYC/CDD checks and verifications as may be necessary in the circumstances.

168. Financial institutions must ensure they can either obtain identification information for the beneficiaries of the accounts or be in a position to confirm that this information can be retrieved on demand. The latter position is predicated on the POC (MLP) Regulations which only permit reliance on third parties where the third Party is itself or himself subject to an AML/CFT regulatory framework. While Attorneys fall in the FATF category of DNFBPs/gatekeepers, the effect of the current injunction[151] obtained in relation to the POCA DNFBP framework is that Attorneys in Jamaica are not yet subject to the DNFBP AML framework in Jamaica.

[150] See also Basel Committee on Banking Supervision – Sound management of risks related to money laundering and terrorist financing – January 2014 – Annex I - Reliance on third parties – Section II

[151] The Jamaica Bar Association successfully obtained an interim injunction in relation to the imposition of the DNFBP framework under the POCA, on Attorneys. The effect of the order is that certain statutory obligations under POCA that apply to the regulated sector (namely financial institutions and designated non-financial institutions - R10, 11, 12, 15, 18, 20, 21, and 24) will not apply to attorneys until a ruling is provided on the substantive matter (i.e. the constitutional motion) which was heard between March 23-26, 2015. All other provisions of POCA remain in effect and applicable to attorneys. The oversight and monitoring framework in relation to the Competent Authority powers regarding the obligations of Attorneys in relation to the aforementioned statutory obligations are also subject to the interim injunction. A copy of the order can be accessed from the website of the General Legal Council at www.generallegalcouncil.org.

Accordingly, when conducting business with an attorney in Jamaica acting as a professional intermediary in respect of any one or more of the matters reflected in the requisite DNFI designation order under the POCA, a financial institution would not be in a position to consider itself entitled to rely on the due diligence processes of an Attorney in Jamaica in accordance with the POCA and TPA until such person are subject to the AML/CFT regime. Accordingly at a minimum a financial institution is required to ensure that:-

(a) Records reflect the particulars of the account holder (i.e. the law firm); signing authorities and persons with the authorization to operate the account;

(b) It accesses and retains the relevant KYC information (as discussed earlier in this section of the Guidance Notes) on account beneficiaries from the law as well as transaction type and payment arrangement).

(c) It conducts its own information verification of source of funds and wealth; ensure advised beneficiaries are not persons on UN list of terrorists or any other list which would suggest that person is a prime suspect for ML or other financial crime); and

(d) It ensures that the operation of accounts is consistent with the advised transaction/(s) or payment arrangement.

PRIVATE BANKING CLIENTS

169. In particular, institutions that offer private banking services for high net worth individuals must ensure that enhanced due diligence policies and procedures are developed and clearly documented in the overall CDD and KYC policies and procedures to govern this area of operations. Senior management with ultimate responsibility for private banking operations should ensure that the personal circumstances, income sources and wealth of private banking clients are known 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 private banking customers and their businesses, these accounts must be available for review by the Supervisory Authority, the Designated Authority, and the financial institution's internal compliance officers and internal

auditors. The approval of private banking relationships must be obtained from at least one senior level officer, other than the private banking officer/relationship manager.

TRANSFERRING CLIENTS

170. Where accounts are transferred from another financial institution, enhanced KYC/ CDD standards should be applied especially if the licensee has any reason to believe that the account holder has been refused banking facilities by the other financial institution.

POLITICALLY EXPOSED PERSONS (PEPS)[152]

171. 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[153] -

(i) heads of state or of government,

(ii) senior politicians,

(iii) senior government officials,

(iv) senior politicians,

(v) senior executives of state owned corporations;

(vi) important political Party officials; judicial or security force and/or military officials (whether elected or not);

(vii) 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)

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

[152] See FATF Recommendation 12

[153] 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.

(b) The 2013 amendments to the POC (MLP) Regulations and TP (Reporting Entities) Regulations defines 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 member of the Judiciary;

(v) a military official above the rank of Captain;

(vi) a member of the police of, or above the rank of Assistant Commissioner;

(vii) 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).[154]

(viii) a director or chief executive of any company in which the Government owns a controlling interest;

(ix) an official of any political Party;[155]

(x) an individual who holds or has held a senior management position in an international organization.

Additional Considerations[156]

172. Given the risk assessment profile requirements under the AML/CFT regulations as well as the risk based approach contemplated by the revised FATF Recommendations, a financial institution would not be precluded from extending the enhanced or heightened measures to persons who are not expressly reflected in the list at regulation 7A(6) of the

[154] This category is interpreted as capturing local government officials from at least the rank of Mayor.
[155] Any member of the Executive of a Political Party.

[156] 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, Ch`arges D` Affaires, Members of the Boards of Central Banks)"

POC (MLP) Regulations and at regulation 6A(6) of the TP (Reporting Entities) Regulations (suach as former PEPs or middle ranking or junior officials acting in the name of, or on behalf of or for a PEP), if from a financial institution'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 or more] of the following-

(a) whether the individual is an elected representative 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 (eg. 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);

(b) the individual's prominence or position (as a prominent public figure) -

(i) 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); and

(ii) 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

(c) the individual meets the criteria of a close associate of a person at a, or b, above.

(d) It should be noted that person who qualify for classification as a PEP can remain subject to an assessment of 'high risk' even after his/her appointment as the basis for such treatment should be based on risk and not on prescribed time limits.[157]

(e) Using a risk based approach presumes that based on the risk assessments conducted, a financial institution would not be precluded from 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. However, currently the

[157] FATF Guidance on Politically Exposed Persons (R12 and 22) June 2013, "B" Time Limits of PEPs Status, paragraph 44, page 12.

AML/CFT regulations already specify the category of persons, who, from a national perspective, are deemed to be high risk[158]. In relation therefore to those specified category of persons, applying reduced or lenient measures should not occur unless that approach is specifically permitted in the AML/CFT laws.

173. Financial institutions should not establish business relationships with PEPs if the financial institutions know or have reason to suspect that the funds derive from corruption or misuse of public assets. Senior management with ultimate responsibility for banking operations should ensure that the personal circumstances, income sources and sources of wealth of PEPS are known 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 Supervisory Authority, the Designated Authority, and the financial institution's internal compliance officers (including the Nominated Officer) and internal auditors. The approval of business relationships involving PEPS must be obtained from at least one senior level officer, other than the banking officer/relationship manager.

174. To mitigate the significant legal and reputational risk exposures that financial institutions face from establishing and maintaining business relationships with PEPS, the following procedures should be followed prior to the commencement of such relationships: -

(a) Information gathering forms/procedures should be structured to reasonably allow the financial institution to ascertain whether a client is a PEP and to identify persons and companies/business concerns clearly related to or connected with the PEP. The financial institution should also access publicly available information to assist in the determination as to whether or not an individual is a PEP;

(b) Confirm the individual's status as a PEP;

[158] 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 2015 corruption perceptions index measures the perceived levels of public sector corruption in 168 countries and territories. In 2015 Jamaica received a ranking of 69 out of 168 or was ranked in the 45th percentile.

(c) Obtain all the relevant client identification information as would be required for any other client prior to establishing the business relationship. Additionally, the decision to open an account for a PEP must be taken at the senior management level;

(d) Assess the nature of the individual's obligations and establish a risk profile for that individual. Even within a designation of 'high risk' it is possible that the specific circumstances of the individual can operate to either substantially mitigate the risks associated with being a PEP, or exacerbate those risks;

(e) Investigate and determine the income sources prior to opening a new account. Reference to income sources includes - source of funds; source of wealth and asset holdings; confirmation of the general salary and entitlements for public positions akin to the one held by the customer in question – (General information on local PEPS may be available from the Public Services Commission in Jamaica. General information on local PEPS can also be viewed from the Jamaica Parliamentarian's Salaries Review Commission Report.[159] This report details – basic salary; and allowances (travelling, subsistence, housing, and utilities.

175. Following the commencement of banking relationships, there should be:

(a) Regular reviews of customer identification records to ensure they are kept current[160]; and

(b) Ongoing monitoring of PEP accounts.

176. The abovementioned 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[161] client base to ensure that all current PEPs have been so identified and remain subject to enhanced customer due diligence processes.[162]

[159] www.parliamentarysalaries.org
[160] POCA (MLP) Regulations, 2007 r. 7(1)(c)
[161] POCA (MLP) Regulations, 2007 r. 19
[162] FATF Guidance on Politically Exposed Persons (R12 and 22) June 2013

NON FACE-TO-FACE CUSTOMERS

177. Financial institutions should avoid the practice of opening new accounts via post, unless higher standards of scrutiny that appropriately address the risks of proceeding are applied. Similarly, accounts opened via the Internet or similar technology, these should be subject to more rigorous identification and verification standards including independent verification by a reputable third Party[163]. (See discussions below on products and services offered through emerging technology.)

At a minimum, financial institutions ensure that[164]:-

(a) Copies of documents presented are certified by the relevant and appropriate authority;

(b) Customers submit additional documents to verify identity; the intended nature of the business relationship, as well as the reason/(s) for the intended or performed transaction/(s);

(c) If possible, face to face contact should be made with the customer by the licensee (eg. Arrange for interviews at their locations where this can be accommodated in a 'best efforts' scenario);

(d) Where third Party introduction is being facilitated, this must be subject to the licensee ensuring that the introducer meets the criteria outlined in the (MLP) Regulations and TP (Reporting Entities) Regulations;

(e) If possible, the first payment is made through a financial institution which has similar customer due diligence standards.

It may also be necessary for financial institutions to increase the number and timing of controls and checks applied during the course of the business relationship including selecting patterns of transactions that will be subject to further examination.

[163] Refer to POC (MLP) Regulations, regulations 7 & 12 ; TP (Reporting Entities) Regulations, regulation 5 & 12
[164] FATF Recommendation 10 – Interpretive Note – paragraph 20.

EMERGING TECHNOLOGY[165]

178. Financial institutions should proactively assess the various risks posed by emerging technologies (For instance, in the use of new payment products and services) and design customer identification procedures with due regard to such risks.

(a) New payment products and services (NPPS) are described in the related FATF Guidance[166] as new and innovative payment products and services that offer an alternative to traditional financial services, and which involve new ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems, as well as products that do not rely on traditional systems to transfer value between individuals or organisations.

(b) Based on the FATF definition of a 'financial institution', the providers of NPPS fall within that definition where the activity occurs through conducting money or value transfer services, or through issuing and managing a means of payment, and according to FATF, should therefore be subject to AML/CFT preventive measures including CDD, record keeping and reporting of suspicious transactions.[167]

Under the BSA, NPPS activities would be captured under the definition of financial services which includes the activities of the transfer of money or value and the issue of electronic money.

(c) Further considerations raised by FATF are that the provisions of NPPS:-

(i) Usually requires a complex infrastructure involving several parties for the execution of payments. This raises a particular concern when it is not, or cannot be clearly established which of the entities involved is subject to AML/CFT obligations and subject to complying with those obligations and

[165] FATF Recommendation 15

[166] FATF Guidance on Prepaid Cards, Mobile Payments and Internet-Based Payment Services, June 2013

[167] Ibid, paragraph 34.

which country is responsible for regulating for compliance with those obligations;

(ii) Sometimes involve the use of agents and reliance on unaffiliated third parties for establishing customer relationships and reloading services which can increase ML/TF risks particularly if the information collected is not shared with the entity responsible for AML/CFT requirements;

(iii) Often involve entities from sectors such as MNOs[168] which are unfamiliar with AML/CFT controls and whose CDD could be limited in comparison to, for eg. the traditional banking sector and in respect of which, the chain of information could create difficulties for tracing the funds involved (for eg. the chain of information for a single transaction could involve more entities, some of which may be located in different countries. (In Jamaica MNOs tend to have major operations on a global basis, and are subject to a regulator whose primary focus is 'market conduct'); and

(iv) Generally involve the maintenance of bank accounts which are used for periodic transactions to settle accounts with agents and MVTs Partners. The issue here is that while a bank settling wholesale transactions between NPPS providers has CDD obligations in relation to the NPPS provider, it has no, or limited visibility into the NPPS providers' customers and is unable to oversee transactions between the NPPS providers and their customers.

(d) The FATF Guidance reflects that examples of emerging new payment methods include:

(i) Prepaid cards, mobile payments, and internet based payments (including virtual currencies). For these activities the risks of ML/TF are increased by the anonymity that can occur when these products are being purchased, registered,

[168] Mobile Network Operators

loaded, reloaded, or used by the customer. These risks are also increased where cash funding, loading or reloading is possible otherwise than through a bank account for example via the internet, or where the technology permits, access benefits are passed on to third parties unknown to the issuer or can facilitate third Party remittances. Products and mechanisms with cash and non-bank payment options open up the payment system access and also obscure the origin of the funds. It is also recognized that the compact physical size of prepaid cards increases the vulnerability of these products being used to effect the cross border transfer of funds i.e. a discreet number of cards that have accounts loaded with high fund values which cannot be determined from the card itself as against transporting large, bulky amounts of cash using cash couriers. The foregoing risks are recognized as being relative to the functionality of the product or mechanism and the existence of AML/CFT risk mitigating measures such as funding or purchasing limits, reload limits, cash access limits and restricting the ability for the product or mechanism to be used outside the country of issue.

179. Given the foregoing, the NPSS' that are high risk and which should be subject to enhanced due diligence measures are NPSSs for which any one or more of the following characteristics is present:-

(a) Where 'airtime' funds can be transferred and are accepted for payments or an alternative currency; or

(b) Where the NPSS is functionally similar to that of a bank account due to the presence of one or more of the following features:

(i) the NPPS can be reloaded an unlimited number of times;

(ii) no or very high funding, loading or spending limits are envisaged;

(iii) it is possible to make and receive funds transfers cross-border, and within the country where product is issued;

(iv) the NPPS can be funded through cash, and cash can be withdrawn through the ATM network; or

(v) the ability to add or withdraw funds to the account using cash or cash equivalents, whether directly or through another provider or intermediary.

(vi) Using agents or unaffiliated third parties to establish customer relationships particularly where the KYC/CDD information is not shared or is not available to, or accessible by, the party with the AML/CFT responsibility;

(vii) Segmentation of the service where one or more unaffiliated third parties are relied on for establishing customer relationships, the issuance or redemption of the currency involved

180. The risks associated with the offer of NPPS may be managed with the application of certain risk mitigating characteristics such as:-

(a) loading solely from a bank account;

(b) absence of funding through third parties;

(c) clear establishment and confirmation of the parties/(ies) with the AML/CFT responsibilities and the country with AML/CFT responsibility (i.e. AML/CFT obligations are statutorily imposed; carry effective, proportionate and dissuasive sanctions for breaches and are equivalent or reflect a higher standard than the AML/CFT laws in Jamaica);

(d) the NPSS party is responsible for handling all aspects of the customer relationship (i.e. registration, cash-in/cash-out and transactions) **and has** AML/CFT responsibility as described above) and is subject to regulatory oversight through a mechanism of licensing or registration; (eg. a NPSS (which operates a MVTS or as a means of payment) who is also a designated DNFI under the POCA)

(e) functionally the following risk mitigating characteristics are incorporated –

(i) CDD Recordkeeping

(ii) Value limits/thresholds

(iii) Geographical limits

(iv) Usage limits (eg. limiting the product to the acquisition of certain goods and services; application of transaction monitoring features;)

(v) Usage safeguards (such as requiring unique identifier information to proceed with a transaction)

181. Where there are multiple entities involved in the provision of the NPPS or service, and it is not clear which entity is the provider, the following factors can be applied in deeming a party the appropriate NPPS provider(s):

(a) the entity which has visibility and management of the NPPS;
(b) the entity which maintains relationships with customers;
(c) the entity which accepts the funds from customer, and
(d) the entity against which the customer has a claim for those funds.

VIRTUAL CURRENCIES[169] ("VC")

182. VC is an example of an internet payment product or service. FATF defines this product as a digital representation of value that can be digitally traded and functions as

(1) a medium of exchange; and/or
(2) a unit of account; and/or (3) a store of value,

but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. It is distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency - i.e., it electronically transfers value that has legal tender status.

183. The FATF Guidance further reflects that virtual currency's global reach likewise increases its potential AML/CFT risks. Virtual currency systems can be accessed via the internet (including via mobile phones) and can be used to make cross-border payments and funds transfers. In addition, virtual currencies commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. This

[169] Guidance for a Risk Based Approach – Virtual Currencies

segmentation of services means that responsibility for AML/CFT compliance and supervision/enforcement may be unclear. Moreover, customer and transaction records may be held by different entities, often in different jurisdictions, making it more difficult for law enforcement and regulators to access them. This problem is exacerbated by the rapidly evolving nature of decentralized virtual currency technology and business models, including the changing number and types/roles of participants providing services in virtual currency payments systems, and importantly, components of a virtual currency system may be located in jurisdictions that do not have adequate AML/CFT controls. Centralized virtual currency systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes. Decentralised convertible virtual currencies allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country[170].
(See pages 10 - 12 of the FATF Guidance for typologies involving the use of virtual currencies.)
(See footnote 4 of the above FATF Guidance which reflects that in addition to AML/CFT issues virtual currency is a complex subject that implicates other regulatory matters, including consumer protection, prudential safety, tax and soundness regulation, and network IT security standards.)

184. VC systems can be traded on the internet, and are generally characterized by non-face-to-face customer relationships, and may permit anonymous funding (cash funding or third-Party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if sender and recipient are not adequately identified[171]. Therefore VC payment products and services ('VCPPS') present money laundering and terrorist financing (ML/TF) risks and other crime risks that must be identified and mitigated.

185. Using a risk based approach presumes that based on the risk assessments conducted, a financial institution would not be precluded from providing relaxed measures for NPPS if the risk assessment confirms that the profile of the product or service or mechanism warrants such an approach to be taken and the appropriate risk mitigating measures are implemented. It should be noted that FATF recommends that the risks posed by NPPS should be identified, assessed and understood before financial institutions seek to establish their CDD processes and procedures and prior to the launch of such services

[170] FATF Guidance on Virtual Currencies – June 2013 – pages 9 &10 "Potential Risks"
[171] Ibid

products or mechanisms. This means looking at the ML/TF risks while the product, service or mechanism is still in its project phase and designing said product, service or mechanism in such a way that the vulnerabilities are kept to a minimum.[172]

In conducting transactions that fall within the parameters of the Electronic Transactions Act, financial institutions should bear in mind the provisions of this Act particularly those treating with the issue of electronic signatures (See section 8 "Requirements for signature"). Financial institutions also bear in mind that Jamaica has legislation in place treating with Cybercrimes[173] and lotto scamming activities and should be cognisant of the obligations and offences described in these pieces of legislation.

CORRESPONDENT BANKING[174]

186. Correspondent banking[175] refers to the provision of banking services by one bank (the correspondent bank) to another (the respondent bank/ other financial entity). The arrangement is used by respondent banks throughout the world to conduct business and access services (such as cash management; international wire transfers, cheque clearing, payable through accounts and foreign exchange services) that they cannot offer directly because of the lack of an international network[176].

(a) Generally, for a correspondent bank, the risks associated with this activity arise:-

(i) where the respondent entity has no physical presence in the jurisdiction in which the correspondent bank is located; and

[172] FATF Guidance for a risk based approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services, June 2013 – paragraphs 61 and 62;
[173] See paragraph 46
[174] See FATF Recommendation13
[175] An example of a correspondent arrangement gone bad – Re: Bank of New York (BONY) Derivative Complaint (Case No. 99 Civ. 10616 (DC) (Con.)) – Amongst the transgressions alleged is that "…Although contemporaneous government, press, and private-sector sources had sounded unmistakable warnings that Russia's nascent private banking system was being infiltrated by organized crime, the BONY Board intentionally or recklessly failed to assure itself that BONY had implemented an adequate and independent system of monitoring and control of its correspondent wire transfer business and Eastern European business operations."

[176] Basel Committee on Banking Supervision – Sound Management of Risks Related to ML and TF, January 2014 – Appendix 2 – general considerations on correspondent banking

(ii) usually because the correspondent bank processes or executes transactions for customers of the respondent but does not generally have direct business relationships with the customers of the respondent bank, as well as the limited information available regarding the nature or purposes of the underlying transactions.

(b) Correspondent banking relationships should therefore generally be subject to the appropriate risk assessment being undertaken in relation to for instance:

(i) The jurisdiction in which the respondent entity is located;

(ii) The group to which the respondent entity belongs and the jurisdictions in which the subsidiaries and branches of the group may be located;

(iii) Information about the respondent entity's management and ownership (especially the presence of beneficial owners), its reputation, major business activities its customers (including target market) and their locations;

(iv) The purpose of the services requested by, or to be provided to, the respondent entity;

(v) Intended usage of the account by the respondent entity, eg. to provide onward correspondent bank services to its own customers; ability of the customers of the respondent entity to directly access the account held by the correspondent bank; to address own corporate or settlement purposes; intended third party usage of the account; to accommodate facilitate or extend 'nested relationships' or payable through accounts.

(vi) The quality of the AML/CFT policies and procedures of the respondent bank (and the CDD applied by the respondent bank to its customers);

(vii) Compliance status with regulatory, prudential and national AML/CFT requirements and global AML/CFT standards;

(viii) The ability to obtain from the respondent bank, the identity of any third party/parties that will be entitled to, or will be accessing or using the correspondent banking services[177];

(ix) The potential use of the account by other respondent banks in a "nested[178]" correspondent banking relationship.

(c) Financial institutions must therefore apply appropriate levels of due diligence by gathering sufficient information from and performing enhanced due diligence processes on proposed respondent banks/ or entities prior to setting up correspondent accounts. This should, at a minimum include: -

(i) Obtaining authenticated/certified copies of Certificates of Incorporation and Articles of Association (and any other company documents to show registration of the institution within its identified jurisdiction of residence) ;

(ii) Obtaining authenticated/certified copies of banking licences or similar authorization documents, as well as any additional licences needed to deal in foreign exchange;

(iii) Confirming the supervisory authority which has oversight responsibility for the respondent bank and its compliance with regulatory, prudential and AML/CFT obligations;

(iv) Determining the ownership of the respondent bank or entity;

(v) Obtaining details of the respondent bank's/ or entity's board and management composition;

[177] Financial institutions should be aware that 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 US to issue a summons or subpoena to any foreign financial institution that maintains a correspondent account in the US and to request records relating to such account, including records maintained outside the US-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. Section 313 of that Act prohibits US banks from establishing correspondent banking relationships with shell banks.
Financial institutions also need to be particularly mindful of the requirements of the USA Patriot Act, which effected several changes to the anti-money laundering and terrorist financing provisions of that country's Bank Secrecy Act.

[178] The use of a bank's correspondent relationship by a number of respondent banks through their relationships with the bank's direct respondent bank to conduct transactions and obtain access to other financial services. Basel Committee on Banking Supervision – Sound Management of Risks Related to ML and TF, January 2014 – Appendix 2 – general considerations on correspondent banking

(vi) Determining the location and major activities of the respondent bank/ or entity;

(vii) Obtaining details regarding the group structure within which the respondent bank/ or entity may fall, as well as any subsidiaries it may have;

(viii) Obtaining proof of its years of operation, along with access to its audited financial statements (for the last 5 years if possible);

(ix) Ascertaining the respondent bank's/ or entity's external auditors;

(x) Ascertaining whether the respondent bank/ entity has established and implemented sound customer due diligence, anti-money laundering and anti-terrorism financing policies and strategies and appointed a Compliance Officer (at senior management level), inclusive of obtaining a copy of its AML/CFT policy, procedures and guidelines;

(xi) Ascertaining whether the respondent bank has in the previous 7 years (from the date of the commencement of the business relationship or negotiations therefore), been the subject of or is currently subject to any regulatory action or any AML/CFT prosecutions or investigations. A primary source from which this information can be sought and ascertained include the Banking Regulatory Authority for the jurisdiction in which the correspondent bank is resident. Information may also be available from the bank's website as well as published information such as the AML/CFT Mutual Evaluation Reports.

(xii) Ascertaining that the respondent banks/ or entities do not permit their accounts to be used by shell banks. In this regard a correspondent bank would also need to pay attention to the following indicators:-

1. whether the respondent bank/ or entity provides intermediary services to its customers such as "payable through accounts"[179], nested relationships or other

[179] According to the FATF (Revised) Interpretive Note to Recommendation 13, the term 'payable-through accounts' refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.

The USA PATRIOT Act Section 311 (1) BANK DEFINITIONS (C) defines PAYABLE-THROUGH ACCOUNT- "as an account, including a transaction account (as defined in section 19(b)(1)(C) of the Federal Reserve Act), opened at a depository institution by a foreign financial institution by means of which the foreign financial institution permits its customers to engage, either directly or through a sub-account, in banking activities usually in connection with the business of banking in the United States."

Section 19(b) 1(C) – The Federal Reserve Act

third party type access to the correspondent accounts. This would be one likely way in which respondent shell banks could take advantage of correspondent banks;

2. the respondent bank's inability or reluctance to provide ultimate beneficiary/customer information in relation to pooled arrangements or collective investment schemes or aggregate accounts whereby only the KYC on the agent of the beneficiaries of the pooled arrangement, collective investment scheme or aggregate account will be or can be provided by the respondent bank;

3. the country in which the respondent bank resides; (see note on countries with inadequate AML/CFT frameworks). Jurisdictions with secrecy laws that

---

(C) The term "transaction account" means a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others. Such term includes demand deposits, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.)

"The arrangement comprising a "payable thru" account usually involves an account service offered by a US banking entity to foreign banks. That is the US banking entity opening a checking account for the foreign bank, and the foreign bank then soliciting customers that reside outside of the US who for a fee, are provided the means to conduct banking transactions in the US through the foreign bank's account at the US banking entity. Typically the foreign bank will provide its customers ('sub-account holders'), with cheques to enable them to draw on the foreign bank's account at the US banking entity." (See FDIC Guidelines on Use of Payable Through Accounts – March 30, 1995 http://www.fdic.gov/news/news/financial/1995/fil9530.html)

US banking entities are mandated to ensure that where payable through account services are provided they-

- Must be able to sufficiently identify the ultimate users of its foreign bank customers' payable through accounts, including obtaining (or having the ability to obtain) in the US substantially the same type of information on the ultimate users as the US banking entity obtains for its domestic customers;

- May be required to review the foreign bank's own procedures for identifying and monitoring sub-account holders as well as the relevant AML statutory and regulatory requirements with which a foreign bank must adhere in relation to customer –related transactions;

- Should terminate the payable through arrangement with the foreign bank as quickly as possible where-
  1. Adequate information on the ultimate users of the payable through account cannot be obtained;
  2. The US banking entity cannot adequately rely on the home country supervisor to require the foreign bank to identify and monitor the transactions of its own customers; or
  3. The US banking entity is unable to ensure that the payable through accounts are not being used for money laundering or other illicit purposes. (www.fdic.gov/news/news/financial/1995/fil9530.html)

prohibit the release of any KYC information or which laws present an obstacle to the KYC due diligence process may pose a particular problem in this regard.

(xiii) Establishing the purpose and interested and expected usage of the correspondent account;

(xiv) Documenting the respective responsibilities of each institution in the operation of the correspondent account;

(xv) Identifying any third parties that may use the correspondent banking services; (in this regard the correspondent bank must be satisfied that the respondent bank has conducted CDD on the customers having direct access to accounts of the correspondent bank and that the respondent bank is able to provide relevant CDD information to the correspondent bank, on request[180]) and

(xvi) Ensuring that the approval of senior management is obtained for the account to be opened.

187. Jamaica currently does not provide correspondent banking services, financial institutions should note however that in the event that correspondent banking services are provided then the financial institution will need to be bear in mind the matters outlined above.

RESPONDENT BANK/ ENTITY

188. Equally important is the respondent bank's/ or entities obligation to ensure that the institution identified to provide correspondent banking services is a reputable one, properly constituted and appropriately regulated. Financial institutions in their role as prospective respondent banks/ or entities , should therefore also note that similar assessments and the due diligence outlined above should be undertaken in relation to the identification of appropriate or suitable entities with which correspondent banking relationships will be established. For respondent banks/ or entities the risk associated with being a respondent bank/ or entity, appear primarily to arise with:-

[180] FATF (Revised) Recommendations, 2012 recommendation 13 paragraph (e)

(a) Establishing a relationship with a correspondent bank which has a poor AML/CFT history and track record and which is subject to sanctions that may result in the funds and other assets held by that entity being frozen which can adversely impact the services of the respondent bank/or entity to its customers as well as the reputation of the respondent bank/or entity in being associated with such a correspondent bank;

(b) Establishing a relationship with an entity which is not licensed; or which has a poor history of regulatory compliance;

(c) Unexpected loss of the correspondent relationship due to the perception that the respondent bank/ or entity is either not AML/CFT compliant, or poses an unacceptable risk to the correspondent bank which can have adverse reputation and operating implications for the respondent bank/ or entity.

SHELL BANKS[181]

189. The FATF (Revised) Recommendations reflect that countries should not approve or accept the establishment or continued operation of shell banks and that countries should refuse to enter into or continue a correspondent banking relationship with a shell bank. FATF defines a 'shell bank' as *"a bank that has no physical presence in the jurisdiction in which it was incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision."*

(a) The BSA, Section 11 prohibits operating as, or having dealings of any kind with, a shell bank. The definition in the BSA also reflects that 'physical presence' is not established by the existence only of any one of the following-

(i) the appointment of a local agent or the employment of non-managerial level staff;

(ii) the presence of resident staff who do not direct the policy and strategy of the bank; or

(iii) the establishment of the bank solely or principally by virtual means.

[181] FATF Recommendations 13 and 26 where the prohibition from operating as or dealing with a shell bank is discussed.

The definition also recognises the power of the Supervisor of banks, financial holding companies and other specified financial institutions, to deem an establishment as one that is consistent with establishment of a shell bank.

(b) To be deemed as having a "physical presence", a financial institution should therefore:

(i) Be physically located (i.e. "brick and mortar "presence) at a fixed address in the country in which it has been licensed to do banking business. This fixed address implies establishment of presence otherwise than by a post office box or electronic address;

(ii) Have mind and management located within the country of operation. (The existence only of a local agent or of non-managerial staff or of staff not authorized or empowered to make decisions and bear legal responsibility for the daily operations of the location, does not constitute physical presence[182]);

(iii) Maintain operating records relating to its banking activities at its fixed address;

(iv) Be subject to inspection by the banking authority by which it has been licensed;

(v) If the entity is a part of a financial group then that should also be a regulated financial group that is subject to effective consolidated supervision.

(c) Financial institutions must undertake the required due diligence (see paragraphs 186-188) to ensure that correspondent relationships are not established or continued with shell banks.

COUNTRIES WITH INADEQUATE AML/CFT FRAMEWORKS[183]

190. As earlier indicated in these Guidance Notes, financial institutions must exercise added care when dealing with clients residing in countries with weak or non-existent laws and regulations to detect and prevent money laundering and terrorist financing, or the financing of proliferation of weapons of mass destruction. A financial institution's assessment and risk based approach regarding the countries flagged or identified as

[182] See FATF Recommendations – General Glossary.
[183] See FATF Recommendation 21

posing AML/CFT risks should be clearly outlined in the financial institution's policy manual and updated whenever necessary. As a general guide in identifying these jurisdictions, financial institutions may refer, to the FATF's list of countries, which have been identified as having strategic deficiencies in their AML/CFT frameworks. Bank of Jamaica will also periodically update its licensees based on advisories received from the CFATF, and on advisories received from the United Nations (through the Ministry of Foreign Affairs and Foreign Trade).

191. The commencement of business relationships with clients residing in countries with inadequate frameworks must be subject to the KYC processes discussed above in Section V and must have the prior approval of senior management. FATF has indicated that possible countermeasures countries can employ to mitigate the risks involved, include the following[184]-

(a) Requiring financial institutions to apply specific elements of enhanced due diligence;

(b) Introducing enhanced relevant reporting mechanisms or systematic reporting of financial transactions;

(c) Refusing the establishment of subsidiaries or branches or representative offices of financial institutions from the country concerned, or otherwise taking into account the fact that the relevant financial institution is from a country that does not have adequate AML/CFT systems;

(d) Prohibiting financial institutions from establishing branches or representative offices in the country concerned, or otherwise taking into account the fact that the relevant branch or representative office would be in a country that does not have adequate AML/CFT systems;

(e) Limiting business relationships or financial transactions with the identified country or persons in that country;

(f) Prohibiting financial institutions from relying on third parties located in the country concerned to conduct elements of the CDD process;

[184] FATF (Revised) Recommendations – Interpretive Note to R19

(g) Requiring financial institutions to review and amend, or if necessary terminate, correspondent relationships with financial institutions in the country concerned;

(h) Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of financial institutions based in the country concerned;

(i) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

192. Under section 94(4)(b) of the POCA institutions are required to pay special attention to transactions involving any customer resident or domiciled in a territory specified in a list of specified territories issued by notice in the Gazette by a Supervisory Authority. Additionally any suspicious transactions originating from, or involving, such countries must also be reported to the Designated Authority in accordance with the POCA.

TRANSACTIONS UNDERTAKEN FOR OCCASIONAL CUSTOMERS[185]

193. An occasional customer (eg. a non-account holder), falls within the definition of 'applicant for business' under the AML/CFT framework. An applicant for business 'means a person seeking to form a business relationship, or carry out a one-off transaction with a regulated business'.[186] Accordingly, a transaction with an occasional customer is subject to the identification and transaction verification procedures, as well as the record keeping requirements and reporting obligations in the law.[187] Where a financial institution undertakes these transactions, satisfactory evidence of identity must be obtained failing which, the transaction should be terminated. If the customer is not an account holder, that customer still remains subject to the CDD and certain KYC requirements set out above, in these Guidance Notes and all copies,

[185]POC (MLP) Regulations, r.6; TP (Reporting Entities) Regulations, r.4.
[186] POC (MLP) Regulations, 2007 r.2; TP (Reporting Entities) Regulations, 2010 r.2.
[187] POC (MLP) Regulations, 2007 r.6 (1)(a); FATF (Revised) Recommendations R10(d). Note that the FATF recommendations (R10) reflect that CDD for occasional transactions should be applied for transactions above the designated threshold of USD/Euro 15000 where there is no suspicion of ML (R10 IN1). Jamaica's requirements are therefore more stringent in this regard as no applicable threshold applies in relation to occasional transactions.

reference numbers and other relevant details relating to the transaction should be recorded and retained by the financial institution for a minimum period of not less than seven (7) years[188].

CUSTODY ARRANGEMENTS

194. A financial institution must take certain precautionary measures in relation to requests to hold boxes, parcels and sealed envelopes in safe custody. Where such facilities are made available to non-account holders, there must be strict adherence to the identification procedures set out in these Guidance Notes and the relevant statutes.

ELECTRONIC FUNDS TRANSFERS (WIRE TRANSFERS, MONEY TRANSFERS ETC.) ACTIVITIES[189]

195. According to the interpretive note to FATF Recommendation 16 – the term 'wire transfer' refers to any transaction carried out on behalf of an originator (natural or legal) through a financial institution by electronic means, with a view to making an amount of money available to a beneficiary at another financial institution (i.e. the beneficiary financial institution), irrespective of whether the originator and the beneficiary are the same person. The following information should be obtained and retained for the statutory period when conducting any electronic fund transfer[190] (EFT): -

(a) The identity of the originator/remitting customer (including name, address and account number (in the absence of an account number, a unique reference number must be included)) whether or not the originator is a customer of the financial institution; {Note that according to the interpretive note to FATF R16, the originator refers to the account holder, or where there is no account, the person who places the order with the financial institution to perform the wire or funds transfer.}

[188] POC (MLP) Regulations, r.14(5)
[189] FATF Recommendation 5 and FATF Special Recommendation on Terrorist Financing
POC (MLP) Regulations, 2007 r.7 and 9
[190] POC (MLP) Regulations, regulation 9; TP (Reporting Entities) Regulations, regulation 9.

(b) particulars (including the identity) of every recipient of the funds transferred (including intermediary recipients) as well as the identity of the ultimate recipient/beneficiary, where practical (including name, address and account number (in the absence of an account number, a unique reference number must be included));

(c) Related messages/instructions that accompany transfers.

196. On the matter of verification of information, institutions through which EFTs originate or are received are required to ensure the requisite originator/ beneficiary information provided is accurate[191] .

197. Given the differing transaction threshold triggers that may be applicable for the capture of such information and the differing information sharing laws and protocols that may be applicable in different jurisdictions, it would be prudent for financial institutions to ascertain certain details or confirmations (see list below) from the counterparty financial institution to be involved in the EFT), ahead of conducting the EFT to ensure that the requirements of regulation 9 of the POC (MLP) Regulations and of the TP (Reporting Entities) Regulations, can be met:

(a) Transaction thresholds at which KYC information described at regulation 9(1) and (2A) of the POC(MLP) Regulations will be captured;

(b) KYC details that can routinely be disclosed in the course of conducting wire transfers; and

(c) Persons from whom disclosures are possible (i.e. originators of the transaction; intended recipients/beneficiaries; and any financial intermediary involved (if one is used).

198. Ascertaining certain information about jurisdiction requirements and practices upfront will also minimize the acceptance of funds transfers in respect of which the relevant KYC details cannot subsequently be obtained, by local financial institutions.

[191] FATF Glossary – "accurate" is used to describe information that has been verified for accuracy.

199. The guidance in this paragraph is applicable to both domestic and cross border EFTs:-

(a) Where a financial institution is not in control of both the sending and receipt of an EFT, then that financial institution is not expected to be in a position to verify the information provided in respect of both the 'send and receipt' aspects of the transaction. However where the financial institution does have control of both the 'send and receipt' aspects of a wire transfer or EFT, then that financial institution must be in a position to verify the accuracy[192] of the information provided in respect of both the 'send and receipt' aspects of the transaction.

(b) Where the information obtained is one which generates or raises a suspicion that ML, TF or breach of the designations regarding the proliferation of weapons of mass destruction is taking place, the financial institution should ensure that the appropriate action is taken (i.e. the transaction is not done and the required disclosure is made as the case maybe).

(c) Batch transfers - Unless the receiving or intermediary financial institution has the technical capability to immediately access from its records, the requisite originator and beneficiary details as discussed above, it should not accept batch transfers regardless of whether such transactions qualify as 'routine' or 'non-routine' transactions.

(d) <u>Transfers not accompanied by the complete originator information</u> –

These transfers should not be processed by the receiving or intermediary financial institution unless and until the complete originator information is available. Where a transfer of this nature is identified, it should be immediately red flagged for either termination or as one not to be acted on, until the requisite information is received. To this end it is the responsibility of financial institutions to ensure that they are legally

[192] FATF Glossary – "accurate" is used to describe information that has been verified for accuracy.

in a position to discontinue or terminate the transaction, or to delay acting on the transaction until the requisite information has been received. In the interest of good customer relations, financial institutions should pursue methods of making customers aware from the outset that all EFTs must be accompanied by the complete originator details as the absence of this information can cause the transaction to be delayed, discontinued or terminated.

(e) Where the receiving or intermediary financial institution finds that there is an ongoing situation of consistent or the frequent receipt of transfers of the nature described in (d) above, it should consider terminating its business relationship with the financial institution from which such transfers are consistently or frequently received (i.e. the sending or ordering financial institution).

(f) The guidance in (c) - (e) above are also equally applicable to financial institutions conducting outgoing domestic or cross border EFTs.

Transactions Conducted through the Society for Worldwide Interbank Financial Telecommunication (SWIFT)

200. SWIFT operates an international financial message system which enables payment instructions between banks involved in an international funds transfer operation[193], and related messages (i.e. statements, foreign exchange and money market confirmations, collections, documentary credits, inter-bank securities trading) to be sent between members and other connected financial institutions all over the world.

SWIFT is solely a carrier of messages. It does not hold funds nor does it manage accounts on behalf of customers, nor does it store financial information on an on-going basis. As a data carrier, SWIFT transports messages between two financial institutions.

[193] Brindle & Cox – Law of Bank Payments – Cap. 3 – pages 64 and 76 - SWIFT is a member-owned cooperative through which the financial world conducts its business operations. Over 8,300 banking organizations, securities institutions and corporate customers in more than 208 countries exchange millions of standardized financial messages through SWIFT. SWIFT has its headquarters in Belgium and has offices in the world's major financial centres and developing markets.

This activity involves the secure exchange of proprietary data while ensuring its confidentiality and integrity[194].

(a) In December 2014, SWIFT introduced a KYC Registry Product for its members. The relevant factsheet on this product reflects that the SWIFT KYC Registry is a global platform to centrally store qualified documents and data that financial institutions can employ while on-boarding, updating or re-evaluating their correspondent relationships. It provides a secure portal for exchanging Enhanced Due Diligence (EDD) and Simplified Due Diligence (SDD) documents and data.

The KYC Registry offers a unique approach compared to current alternatives by providing access to a standard set of due diligence documents and data. All information in The KYC Registry undergoes exhaustive quality control and transparent validation by a dedicated operational team at SWIFT. Each Registry user retains ownership of its data. Registry users can only access each other's data when permission to do so has been granted by the data owner.

(b) The SWIFT Traffic Profile is a unique, value-added report that SWIFT offers in connection with The KYC Registry. It uses aggregated global payment data to help banks pinpoint areas of potential risk from specific jurisdictions and supports due diligence activities by providing an independent, fact-based overview of a specific bank's direct and indirect/nested correspondent banking activities.[195]

The relevant fact sheet specifically reflects that SWIFT has no involvement in any type of judgmental activities such as due diligence, screening, risk scoring or recommendations about the closure of business relationships as those remain the responsibility of the financial institutions that use the Registry.

[194] See the SWIFT website at *www.SWIFT.com*
[195] complianceservices.swift.com/kyc-registry

(c) Local financial institutions that are participants in SWIFT therefore remain ~~are~~ mandated to apply full KYC and enhanced due diligence requirements as participating in SWIFT or the SWIFT KYC Registry initiative is not an alternative to this requirement.

ANONYMOUS ACCOUNTS/ ACCOUNTS IN FICTITIOUS NAMES/ NUMBERED ACCOUNTS[196]

201. A financial institution must not in the course of business carried on by it, permit any person with whom it forms a business relationship, to conduct any transaction with it by means of an anonymous account, an account held in a fictitious name[197] or an account identified only by a numbered account.

(a) An anonymous account includes an account for which there is no name, by which the account holder can be identified. That is to say that in relation to such an account, even when that account is subjected to the identification and transaction verification processes outlined under the POC (MLP) Regulations; the identity of the account holder is still not satisfactorily established.

(b) A numbered account refers to an account that is identifiable solely by reference to the number or series of numbers assigned to that account.

(c) An account held in a fictitious name includes an account name which when subjected to CDD identification and verification procedures, does not constitute the true name of the account holder or of the Principal on whose behalf the transaction is being done, or of the beneficiary of the legal arrangement through which the transaction is being conducted.

[196] Regulation 16, POCA (MLP) Regulations and Regulation 16, TP (Reporting Entities) Regulations
[197] FATF Recommendations 9 and 10; Sections IV above.

Specific ADDITIONAL Guidance for Cambios, (Exchange Bureaux) and Money Transfer and Remittance Agents and Agencies (Remittance Service Providers (RSPs)/Remittance Companies)

202. This section provides additional guidance on the identification and verification procedures that cambios and remittance companies are required to undertake before proceeding with a transaction or before establishing a business relationship. It is understood and accepted that the nature of the relationship between cambios, remittance companies and their respective customers can be fundamentally different from that established between banks and other regulated financial institutions and their customers. Cambios are entities, which are permitted with the approval of the Bank of Jamaica, to buy and sell foreign currency only. Remittance companies are entities which facilitate the movement of funds from one person to another person (whether intra-island or across national borders) by way of remitting the funds from one remittance company to the next location of its remittance arm which bears proximity to the destined location of the intended recipient outlined in the customer's instructions. The customer profile of cambios and remittance companies will therefore fall largely within the following categories: -

(a) Customers[198] conducting one-off transactions;

(b) Customers constituting visitors to the country (i.e. tourists / visitors on business (entertainment/sporting events); persons in Jamaica on work permits etc.)

(c) Repeat customers which for the purposes of these Guidance Notes means the following:-

(i) Repeat customers, for the purpose of cambio transactions, are "Persons who conduct a US$250[199] and over transaction or its equivalent in other currencies, more than once in a three (3) month period".

[198] Customers – both individual and corporate

(ii) Repeat customers, for the purpose of outbound remittance transactions, are defined as "Persons who transact business with a Primary Agent (and/or the sub-agent/(s) thereof) more than once within a three (3) month period irrespective of the transaction amount".

Based on the customer profile of these entities there may be practical difficulties with enforcing the same level of KYC procedures in relation to the customers described above particularly in relation to (a) and (b).

203. The interpretive note to FATF R16 (wire transfers) reflects that money value transfer operators should be subject to all the requirements of FATF R16 on wire transfers in the countries in which they operate, whether these operations occur directly or through agents. The KYC and CDD requirements reflected in these Guidance Notes are therefore fully applicable to cambios and remittance companies.

However, considering the typical customer profile of cambio and remittance businesses, it might not in all cases be practicable or feasible for the methodology applied by banks and banking institutions as regards establishing KYC procedures to be fully applicable to all cambios and remittance company transactions. Consequently, cambios and remittance companies will have to employ measures which are more compatible with the nature of the relationships generated by such businesses (whether customer-related or otherwise) to obtain CDD and KYC information. (One example of this is the Corporate Profile form developed by the Cambio Association of Jamaica in consultation with the Bank of Jamaica)

KYC GUIDANCE

204. As cambios and remittance companies largely operate on a 'one-off' transaction basis and 'walk-in- customers' environment, these persons are not expected to apply the exact verification procedures that may be possible for other financial institutions which can establish account holding relationships with their customers. However, cambios and

[199] Or the equivalent of US$250 in any other currency.

remittance companies are expected to employ verification processes more suited to their operations in order to satisfy themselves of the veracity of the information provided and of the authenticity and validity of the identification tendered. (Techniques to be employed may include but not be limited to checking the signature of the applicant for business with the signature on any transaction instrument or documentation offered by the customer; ensuring that identifications tendered are current and do not appear to be forged documents or documents that have been tampered with; that the picture in the identification used is consistent with the features of the person tendering the identification; questioning the customer for confirmation details where this becomes necessary in the circumstances and clearing all cheque transactions before proceeding to act upon such instruments.)

205. Transaction verification efforts that involve checking the nature of the transaction against the risk factors indicated below may also be employed to assist with a determination of the genuineness of the transaction.

(a) Transaction is unnecessarily complex for its stated purpose.

(b) Transfers being made on behalf of a third party.

(c) Transaction is inconsistent with financial standing or occupation indicated, or is outside the normal course of business for the customer in light of the information provided by the customer;

(d) EFT transaction:-

(i) involves EFT to one or more foreign countries with which there is no clear or apparent connection;

(ii) involves Transfers to the same person from different individuals or to different persons from the same individual;

(iii) involves EFTs not accompanied by complete originator information

(iv) does not appear to match the recipient's usual needs or receiving pattern.

(e) Unusual currency exchange (*e.g.* small denomination currency for high denomination currency; or transaction requested seems inconsistent with the customer's expected requirements based on the information provided by that customer).

Additional MVTS ('Money Value and Transfer Services') (this sector includes RSPs) related operating risk factors can be found in the FATF Guidance- for a risk based approach Money or Value Transfer Services, February 2016, paragraphs 47-50.

206. For inbound EFTs beneficiary institutions, are required to ensure that all relevant KYC and CDD information pertaining to the sender (originator of the remittance) as well as the beneficiary (ultimate recipient of the remittance) is obtained but the verification of the information pertaining to the sender (originator) is the responsibility of the institution from which the remittance is sent or originates (the ordering institution). There is a responsibility however to obtain and verify all information pertaining to the ultimate beneficiary of the remittance proceeds who in this scenario, is the customer of the beneficiary institution. [200]

207. For transactions with cambios and remittance companies amounting to, or exceeding USD1,000, identification and documentation pertaining to the source of the funds used in the transactions that are tendered must be copied and the copies retained for the records of the cambio / remittance company. POCA also requires that EFTs exceeding this threshold of USD1000, must also include the national identification number; customer identification number and the originator's date and place of birth. The date and place of birth of the account holder from whose account the funds involved in the EFT originate, must also be provided.[201]

208. All repeat customers must submit the requisite KYC and CDD information including documentation pertaining to the source of the funds used in the transaction regardless of the transaction amount.

209. The applicant for business/customer identification requirements could be considered to be satisfied where the applicant for business/customer identification is an Authorized Foreign Exchange Dealer or a Cambio, unless the transaction is red flagged for closer scrutiny or the transaction amounts to a suspicious or unusual transaction.

Comment [RH8]: Exemption for authorized dealers (i.e. persons who are regulated DTIs and cambios). DTIs are subject to the following exemptions:-
(a) identification procedures at reg. 7 by virtue of Regulation 10 POC (MLP) Regulations and TP (Reporting Entities) Regulation;
(b)de minimis provision at reg.8 and
(c)cash transaction limits at section 101A.

cambios are currently subject to the following exemptions:-
(a) de minimis provision at reg.8 and
(b) cash transaction limits at section 101A.

But money service businesses (which definition includes cambios) are globally flagged as high risk businesses primarily because they tend to be cash intensive. The POCA however does not name MSBs as a high risk area. Should this impact the current practice reflected in the G. Notes from 2004 of relaxing requirements where the applicant for business with a MSB is another MSB (i.e. a cambio)?

NB. Payments from an applicant for business made via accounts held in the name of the applicant for business with a DTI or cooperative society (i.e. credit union), are deemed to constitute the required evidence (verification) of identity for the purposes of regulation 7. Legal discussions on the matter indicate that the definition of a payment may be in practice different from access to funds obtained via funds transfer or wire transfer. This could mean that possibly, the regulation 10 exemption from satisfactorily establishing identity through the procedures outlined in regulation 7, may not be applicable to regulation 9 wire and funds transfers requirements.

[200] FATF Revised Recommendations Interpretive Note to R16 – Paragraph E – Responsibilities of Ordering, Intermediary and Beneficiary Financial Institutions. Paragraph F on Money or Value Transfer Service Operators reflects that these persons should be required to comply with all the relevant requirements of R16.
[201] Regulation 9(2A), POC (MLP) Regulations, amended 2013

210. In the case of body corporates doing business with cambios, the information requirements of paragraph 131 (c), (d), (f), and (g) – will be satisfied if the corporate customer completes and submits to the Cambio with which business is to be transacted, the Corporate Profile Form. The minimum financial information that cambios should obtain from corporate customers are:-

(a) Total Capital as at the end of the last financial year for the customer;

(b) Total Assets as at the end of the last financial year for the customer;

(c) Total Liabilities as at the end of the last financial year for the Customer;

(d) Change of Directors/Principals/significant shareholders/ signing officers/ since the completion of the last corporate profile form;

(e) Main business to be carried out/services to be offered by the customer;

(f) Whether the customer is in possession of any special authorizations under the BOJ Act Section IVA pertaining to foreign exchange activities; (Details of the authorization and duration thereof are to be provided if the customer indicates such authorization exists);

(g) Purpose of FX activities the company expects to conduct with the cambio i.e. –

(i) Bill payments for services rendered by overseas based parties; or for items purchased from overseas for the customers own use;
(ii) Importation of commercial goods;
(iii) Own account investment activities;
(iv) Other (details to be provided as to what the activity entails)

In outlining the purpose of the FX activities to be conducted, a general estimation of the frequency with which the company expects to be conducting or actually conducted these activities for the relevant period to be included eg. daily; weekly; fortnightly; monthly; bi-monthly; quarterly; bi-yearly; annually; occasionally; or as the need arises.

211. For the purposes of the additional guidance for cambios and remittance companies in these Guidance Notes, a "*significant transaction*" which is defined in Section V of these Guidance Notes includes any transaction amounting to or exceeding US$8,000 (in the case of business done with cambios) and US$5,000 (in the case of business done with remittance companies) or the equivalent thereof in any other currency. Accordingly –

(a) In addition to the copies of identification and source of funds information that must be obtained, and retained, the more fulsome KYC particulars and as far as possible verification processes akin to those outlined in Section V, applied; and

(b) Transaction purpose must be documented (copies of documents which explain or outline the transaction should also be obtained and retained) and the transaction should be subject to further reviews :-

(i) obtaining and verifying additional information on the customer from wider sources and reviewing the customer's profile;

(ii) more rigorous review of the customer's background (financial, professional and personal as far as is reasonable)

(iii) subjecting transaction history information to consistency checks with earlier information provided and new information provided by the customer; and

(iv) looking at customer's willingness to provide sources to allow for independent verification of information supplied to the cambio or remittance company;

(v) ascertaining the reason for conducting the transaction with a MSB as against a bank; and

(vi) whether the transaction was attempted elsewhere and refused and the reasons for that refusal

Implementation is perhaps better accommodated by establishing minimum advance notification requirements for customers intending to conduct a significant transaction to allow the information to be provided to the cambio or remittance company and the requisite verification to be undertaken prior to the transaction being facilitated.]

Cheque Transactions

212. As regards the process of ensuring cheques are cleared before acting on them, cambios could consider that there are inherent risks generally associated with the presentation and clearing of cheques because a collecting bank is unable to verify the genuineness of a cheque, or ascertain the availability of funds at the time of accepting the deposit. For purposes of the Clearing House rules there is no distinction between a Manager's Cheque and personal or company cheques. A commercial bank therefore has the discretion to make a credit decision to release funds sooner depending on the customer's circumstances, however the incidence of frauds perpetrated against banks with the use of manager's cheques has caused many banks to discontinue exercising their discretion in this manner. Cambios and remittance companies which therefore make the business decision to advance funds to customers against cheque payments should note that they do so at their own risk of the cheque not being paid.

213. Cambios and remittance companies should consider employing the following measures when conducting cheque-related transactions-

(a) Ensuring sight of sufficient documentation to satisfy the cambio/remittance companies that the cheque tendered is the result of a genuine transaction with a commercial bank (eg. sight of passbook and copying the receipt tendered as being that issued by the bank (whether via ATM or over the counter)); or

(b) Contacting the issuing bank to confirm the fact that the cheque was drawn on the bank and cros checking details to establish a reasonable level or degree of certainty that the transacting customer is the genuine party authorized to be transacting business with that cheque; and

(c) Ensuring the cheque is subjected to inspection to determine whether it is technically in order which includes inspections to determine that:

(i) The cheque is properly signed;

(ii) The cheque is properly dated;

(iii) Numbers and figures correspond;

(iv) There are no unsigned alteration/s;

(v) Other essential features are present(eg. serial number of the cheque; code identifying the branch of the paying bank on which the cheque is drawn) etc; and

(c) Employing the following operational measures to limit exposures to cheque-related transactions-

(i) Limiting acceptance of cheques subject to third party arrangements as obtaining clearance for these cheques would be significantly more difficult than for cheques that are direct (i.e. payable to the cambio or remittance company, or to the person tendering the cheque);

(ii) Limiting acceptance of personal cheques as the same difficulty above arises in these circumstances;

(iii) Applying transaction limits for cheque-related transactions;

(iv) Refusing to conduct cheque-related transactions in circumstances where the transaction is so out of the ordinary course that it raises doubts about the genuineness or accuracy of the transaction (eg. cheques payable to a company being tendered by that company's agent for a cambio transaction), or it appears that the bearer's title to the cheque may be defective, or it appears to be a transaction in respect of which a disclosure under section 94 or 95 of the POCA or under section 16 or 17 of the TPA should be made.

Customer operating through a Bearer or Agent

214. Where the applicant for business is a corporate customer seeking to act through an agent/bearer (whether employed or contracted) the cambio or remittance company must also enforce the customer identification requirements in relation to the agent/bearer. Additionally, the agent/bearer must submit a copy of the corporate customer's certificate of incorporation and a letter from the corporate customer on the corporate customer's

official letterhead and bearing the signature of an authorized officer.[202] The letter should clearly indicate the business to be transacted, that the agent/bearer is acting on the corporate customer's behalf for this matter and that the person signing to the letter is authorized so to do. Where in relation to the corporate customer it appears to the cambio or remittance company conducting the transaction that the agent/bearer is not the usual agent/bearer, or the letter from the corporate customer is in any way defective, (eg. it is not on the official letterhead; there have been alterations or amendments to the contents of the letter which are not signed by the author of the letter; or the letter itself is not signed) business should either not be transacted at all, or should be delayed until the corporate customer is contacted by the cambio or remittance company and asked to confirm in writing or issue renewed written instructions and the confirmation or renewed instruction is in fact received. Even in the absence of these warning signals cambios should, as a matter of course, employ the practice of conducting random checks with the corporate customer to satisfy itself of the genuineness and accuracy of the transaction to be conducted.

(a) Similar practices should be employed for agents or bearers acting for individual customers.

Establishing Appropriate Identification

215. The "appropriateness test" of the identification obtained is that, from the records prepared and retained by the cambios or remittance companies, one should be able to compile a complete picture of the customer and of the business that customer transacted with the cambio or remittance company.

216. The type of identification tendered must be any one of the options described at paragraph 119 above. If an applicant for business has none of these forms of identification with him/her, then the cambio or remittance company may consider relying on the options outlined above in paragraphs 120-121. Additionally the cambio could accept a customer's client card (where the client card was issued to that customer by the specific cambio or

[202] For the purpose of these Guidance Notes "authorized officer" would mean a manager /senior officer of the company, and as such the letter should clearly indicate the name and position of the "authorized officer".

remittance company itself). Where however client cards are the sole source of identification relied on, the Cambio's records or the records of the remittance company must contain a photocopy of the customer's official identification as well as corroboration of the customer's address and source of funds and these records will need to be updated from time to time (see paragraph 117 above); or accept:-

(a) a birth certificate accompanied by a Declaration of Identification and a photograph both of which (i.e. the Declaration and the photograph) must be signed by a Justice of the Peace (JP), a Minister of Religion or an Attorney-at-Law, to whom the customer is personally known, and who is reasonably capable of confirming the identity of the customer; (This identification evidence should be collected from the customer and retained by the cambio/remittance company and the reference number on the birth certificate clearly indicated on the document evidencing the transaction and the Declaration and copy birth certificate stapled to the document evidencing the transaction.)

(b) In the case of Remittance Companies when conducting inbound transactions only, with a customer who is a student, a valid school ID, where the student customer is enrolled in a secondary or tertiary institution, may be accepted where the student customer identified as the recipient beneficiary, is maintained through remittances sent by overseas parents or guardians responsible for him/her. The ID must have the features outlined in paragraph 119.

(c) The customer's **complete** residential address must be recorded. Therefore short addresses such as May Pen P.O. or Post District PA; will **not** be acceptable. The address must be sufficient for the customer to be contacted by mail or by hand (i.e. bearer) and (should the need arise) by telephone (see note further down). If a business address is being given as the official address of contact (where the applicant for business is a corporate customer) then the name of the business should also be given and the full business address stated. Descriptions such as "business place" will not be acceptable. If there is any uncertainty about the address, a contact number must be obtained from the customer.

It is likely the customer base for a cambio or remittance company is likely to have a higher incidence of persons falling within the category of persons reflected at paragraph 120 above. Accordingly, the assumption discussed at paragraph 123 regarding a financial institutions reliance on the exceptions as the normal acceptable identification as acting contrary to its KYC obligations will not apply to cambios and remittance companies unless the reliance occurs outside the parameters outlined in paragraphs 120-121 and paragraphs 216 – 217 of these Guidance Notes.

Suspicious Transactions

217. It should be noted that paragraphs 27 and 28 above are also applicable to cambios and remittance companies. Where a transaction appears to be one in relation to which a disclosure should made pursuant to section 94 or 95 of the POCA (i.e. suspicious), or pursuant to section 16 or 17 of the TPA, the transaction should not be conducted. Transactions that are not at the stage of being regarded as suspicious but which appear unusual, and therefore raise questions or are flagged for closer scrutiny and which in that case are still conducted, should be subject to full KYC banking standards and reported to the Designated Authority in accordance with the POCA or the TPA (where applicable).

The ability to discontinue transactions or terminate business relationships.

218. As cambios and remittance companies will not be opening or operating on-going accounts for customers, it may be unlikely that prolonged business relationships such as those established with customers by other financial institutions, (banks, insurance companies, unit trusts, mutual funds, securities dealers, cooperative societies), will be established in the case of cambios and remittance companies. Cambios and remittance companies must nonetheless seek to employ procedures that make it **abundantly clear** that they can refuse to do business with a customer and this is probably best achieved by a bold notice to this effect being displayed perhaps by the window of the teller. In the case of persons who have obtained client cards, the documentation issued with the card or the card itself should make it abundantly clear that the card privileges and the card can be

withdrawn at anytime without notice where the cambio or remittance company believes that its discretion in this regard needs to be exercised.

SPECIAL GUIDANCE REGARDING TREATMENT OF LISTED ENTITIES

219. Financial institutions are required to determine whether they are in possession of property for persons on the U.N. lists of terrorists or persons linked with terrorists (refer to section 15 of the TPA). Financial institutions are further required to flag accounts where these are held in the names of persons included on the above referred U.N. lists, and to report the matter to the FID.

Institutions should note that once a person has been designated a 'listed entity", by order of the Supreme Court in accordance with s.14 TPA, this designation will be published by the DPP in a daily newspaper in circulation in the Island. Since the passage of amendments to the TPA in 2011, the following printed publications pursuant to section 14 of the TPA have been made:-

(a) Supreme Court order dated June 6, 2012 approving the designation of persons included in the UNSCR Sanction Committee's list SCA/2/11(20), SCA/14/12(2) and SCA/2/12(03) list of terrorists as 'listed entities'1267 Committee's list of terrorist as 'listed entities'.

(b) Supreme Court order dated July 12, 2013 approving the designation of persons included in the UNSCR Sanction Committee's list SCA/14/13(3) and SCA/2/13(5) list of terrorists as 'listed entities' and updates to the UNSCR 1267 Committee's list of terrorists as 'listed entities'.

(c) Supreme Court order dated March 13, 2014 approving the designation of persons included in the UNSCR Sanction Committee's list SCA/12/13(33) and SCA/14/13(11) list of terrorists as 'listed entities' and requisite updates to the UNSCR 1267 Committee's list of terrorist.

220. Financial institutions may find that they are in possession of property for, or in relation to, the following:-

(a) Persons affiliated/connected[203] with listed entities; (i.e. the customer is a director, or shareholder of a company that is connected with the listed entity; or the customer includes the listed entity as one of its trading Partners; customers; investors; consultants; etc.)

(b) Persons for which the names are very similar to those appearing on the list of listed entities (i.e. constituting a 97% match, for example, in the case where individuals' Christian/First Names and Surnames match but Middle Names are different; or where Full Names match but the customer is female whereas the person on the listed entity list is identified as male; in the case of incorporated/unincorporated entities, the names are sufficiently similar to consider that entity a related entity; or the name constitutes the English version of the name on the listed entity list);

(c) Persons whose business documentation reflect that commercial activities are conducted in territories that are generally featured as "generators or producers of terrorists"; or "sympathetic to terrorists" as indicated in official advisories from the U.N.; FATF; Ministry of Foreign Affairs and Foreign Trade; Designated Authorities (viz AML/CFT typologies); or the Competent Authority;

(d) Persons resident or domiciled in a territory specified in a list of applicable territories published by notice in a Gazette by a supervisory authority[204].

221. It is likely that the view might be formed that transactions/accounts with such persons may not be at the stage of being regarded as suspicious but do in fact raise questions. These accounts or transactions should be flagged for closer scrutiny and subject to

[203] '*Connected/affiliated'* has the same meaning as defined in the BSA
[204] The POC (Amendment) Act, 2013 Section 94(4). As signatories to various UN Conventions and CFATF, it would seem that Jamaica may need to ensure that jurisdictions that are flagged or blacklisted by the UN or CFATF should be included in a gazetted Notice.

enhanced due diligence checks. For example if the scenario at 220(b) should exist, the institution should consider taking steps to ascertain date of birth information; customer gender and possibly have the customer come in to the financial institution with a view to updating the KYC information on file. Scenarios at 220(c) and (d) may require the institution to link with an industry representative body within the jurisdiction from which the documentation originated (such as the Bankers' Association), with a view to ascertaining guidance on how checks can be done to satisfy the institution of the bona fides of the documentation. Where the business relationship is continued or the transaction is conducted, the account or transaction should be subject to KYC standards and additionally reported to the Designated Authority without delay. Resorting to full KYC checks in such circumstances means conducting enchanced due diligence and independent verification of information received in addition to any reliance on the due diligence that may have been undertaken by the originator of the transaction documentation.

222. While cambios and remittance services do not hold accounts or assets for their customers (such as bank accounts, investment accounts or any other ongoing entitlements) these persons would still be required to file a report under section 15, TPA. In most cases these persons would probably be filing a 'nil report' pursuant to section 15(3)(a) – "*that it is not in possession or control of any property referred to in subsection 15(2)"*. It is also possible a cambio or remittance service may be in a position to file a report under section 15(3)(b) *"that it is in possession or control of such property, in which case it shall also report the number of persons, contracts or accounts involved and the total value of the property."*– One such circumstance could possibly arise where the cambio or remittance service provider retains possession of negotiable instruments (i.e. money order, and cheques, which are not 'bearer instruments' and which have been accepted from a customer in the course of conducting a transaction. This point is only made to reflect that cambios and remittance services still need to review their transactions to determine whether a report is required under section 15(3)(b), TPA as against 15(3)(a), TPA.

SPECIAL GUIDANCE - UNSEC RESOLUTIONS ON THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

223. Financial institutions:-

(a) must ensure due diligence programmes, policies, procedures and controls established pursuant to AML/CFT obligations[205] also incorporate measures to allow for the identification of high risk customers and transactions in relation to the DPRK and DPRK banks (including branches and subsidiaries).

(b) Should ensure that the due diligence measures at (a) make similar allowances for Iran and any other jurisdiction designated by the UNSEC or the Sanctions Committee of the UNSEC (including correspondent accounts or relationships such as joint ventures or jointly owned banking operations or facilities with Iranian banks (including branches and subsidiaries)).

(c) Should note that the financial sanctions outlined in the successor resolutions to the UNSEC Resolution 1737(2006) in relation to Iran, highlight 2 banks[206] in particular (Bank Meli and Bank Saderat and extend to the Central Bank of Iran[207];

Noncompliance with the requirement at 223(a) will constitute a breach of the Supervisory AML/CFT Rules.

[205] Regulation 5 of the POC (MLP) Regulations
[206] UNSEC Resolution 1803(2008) (Paragraph10)
[207] UNSEC Resolution 1929(2010) (page 3)

224. Where, after November 15, 2013[208], freezable assets or 'dealings' have been identified (whether in the form of accounts established, funds held, transactions facilitated, lines of credit established; wire transfers accommodated (whether inbound or outbound) or otherwise, then, in relation to the DPRK :-

(a) the requisite reporting should be done to the CTD of the FID; and

(b) an application should be done to the Minister pursuant to regulation 7 of the Regulations either requesting that the financial institution be permitted to use or deal with the freezable asset in a specified way (eg. honouring contractual obligations to the point where termination or discontinuation of services or activities can be undertaken without penalty or without prejudicing the rights of a bona fide third Party or counterparty) or to permit the asset to be made available to the designated entity (eg. return of funds to the account holder if an account is closed).

(c) A copy of the application to the Minster should be provided to the CTD of the FID and when a response to that application is received by the financial institution, a copy of that response should also be provided to the CTD of the FID.

225. In between the identification of freezable assets or dealings with freezable assets and obtaining written notification to use or deal with the assets in a specified way, a financial institution could be liable to prosecution because holding, using or dealing with freezable assets, is an offence of strict liability.[209] It is therefore imperative that a financial institution employs the requisite checks to ascertain whether or not it is in possession or control of freezable assets as quickly as possible. Once such assets have been identified, any dealings that occur in relation to such assets should immediately be contained to the sole purpose of preserving the value of such assets. Regulation 5(3) stipulates that it is a defence against a charge under regulation 5, if the person charged proves that the use or dealing was solely for the purpose of preserving the value of the freezable asset.

[208] Date of Assent to the UNSEC Act, 2013
[209] Regulations 5(3) and 6(3), POC (MLP) Regulations

Financial institutions should note that in relation to a charge under regulation 6 (directly or indirectly making a freezable asset available to a designated entity), strict liability will not be applicable in circumstances where the dealing in question has been permitted by written notice under regulation 7.

226. Where, after November 15, 2013[210], in relation to Iran or such other jurisdiction identified by the UNSEC as a jurisdiction in respect of which targeted financial sanctions should be imposed, freezable assets or 'dealings' have been identified (whether in the form of accounts established, funds held, transactions facilitated, lines of credit established, wire transfers accommodated (whether inbound or outbound) or otherwise, then, in the absence of implementing regulations, a financial institution should:

(a) Where it is determined that this can be done without any or with manageable legal repercussions, consider take the following steps:

(i) confine any dealings in relation to such assets to the sole purpose of preserving the value of such assets;

(ii) bring the matter to the attention of the Minister in writing for the purpose of having the injunctive powers through the Attorney General invoked pursuant to section 7 of the Act; and

(iii)report the holding or dealing of the freezable asset to the CTD of the FID; or.

(b) Without delay, obtain the requisite legal advice as to the extent of their possible liabilities or exposure and as to the available courses of action to effectively minimize this risk and the risk of prosecution.

[210] Date of Assent to the UNSEC Act, 2013

ADDITIONAL GUIDANCE - FINANCIAL HOLDING COMPANIES

227. With the 2013 amendments to the POCA, the Fourth Schedule thereto extended the category of 'regulated business', to include Financial Holding Companies and therefore now refers to "*an entity with corporate responsibility for the development and implementation of group wide AML/CFT policies and procedures for the group of entities of which it forms a part."* Accordingly a financial holding company or such other person bearing this responsibility is fully subject to the statutory AML obligations under the POC legislation.

A financial holding company is also subject to the mandates outlined in Section IV above and especially paragraphs 87-91, 228-229 in relation to local and overseas branches and subsidiaries.

ADDITIONAL GUIDANCE - BRANCHES AND SUBSIDIARIES

228. In complying with the mandates at Section IV above in relation to local branches and subsidiaries and the corresponding mandates under the POCA and TPA in relation to overseas based branches and subsidiaries, a financial institution shall in relation to its subsidiaries and branches, ensure –

(a) the KYC details for customers are well documented (i.e. identification and other customer information as defined under the POCA (MLP) Regulations,) is submitted and recorded); source of wealth is obtained as a part of the financial history of the customer as well as transaction details (including nature of the transaction, transaction amount; currency used; method of payment [cheque/cash/credit card/debit card/wire transfer] and source of funds used to make the payment) are recorded;

(b) AML/CFT internal regulatory controls (i.e. employee training; designation of a nominated officer; auditing of internal controls etc.) are documented (where applicable), approved and implemented;

(c) required disclosures (i.e. STRs) are made and any other reporting obligations are met;

(d) AML/CFT measures are employed in a risk based manner. (eg. processes that include the imposition of transaction limits beyond or below which enhanced or reduced monitoring measures may be applied; and in relation to branch and subsidiary operations[211] in Jamaica, measures that track cash transactions are implemented as such transactions facilitate anonymity in relation to financing of transactions and source of funds.

229. A failure to carry out these requirements will constitute a breach of the BOJ's AML/CFT Supervisory Rules.

ADDITIONAL GUIDANCE - AGENT BANKS

230. A deposit taking institution under the BSA which has appointed an agent pursuant to the BSA shall in relation to that agent, be subject to the same mandate as outlined at Section IV above in relation to its branch operations. (See Additional Guidance- Branches & Subsidiaries)

[211] Agents not included. POCA exemptions from cash transaction limits (s.101A) apply only to banks or DTIs licensed and regulated by BOJ and cambios; or persons specifically exempted by the MNS. Agents are persons authorized to undertake some banking services for appointing DTIs but that authorization does not equate to a licence. Nor can an agent undertake banking services in its own right.

231. In this regard, an agent found to be operating in breach of the AML/CFT policies and procedures of its appointing deposit taking institution shall be in breach of the AML/CFT Supervisory Rules.

An appointing deposit taking institution whose agent is found to be operating in breach of the appointing deposit taking institution's AML/CFT policies and procedures shall also be in breach of the AML/CFT Supervisory Rules.

A breach of the AML/CFT Supervisory Rules may result in the removal/ revocation of the appointing deposit taking institution's approval to offer agent services.

SECTION VI – THE NOMINATED OFFICER REGIME

REPORTING OBLIGATIONS AND THE APPOINTMENT OF NOMINATED OFFICERS

232. **Appointment of Nominated Officers**[212] - A financial institution must designate an officer of the institution who performs management functions as its "Nominated Officer", to be responsible for ensuring the effective implementation of the established policies, programmes, procedures and controls to prevent and detect money laundering and terrorist financing activities in accordance with the relevant statutes, the BOJ Guidance Notes and the licensee's own policies and procedures.

233. In practice the function of nominated officer is most effective if that function is a position that:-

[212] See POCA (MLP) Regulations, 2007 r. 5(3); TPA section 18(3)

(a) is sufficiently senior to allow for reporting to the Board, (or such other governing body by whatever name called) of the institution either directly (at Board meetings) or through a sub-Committee of the Board, on the institution's AML/CFT compliance[213];

(b) requires an awareness of the AML/CFT laws, framework, global practices and trends that can guide the institution in establishing and maintaining the requisite controls, policies and procedures in accordance with the statutory requirements and related framework;

(c) requires the ability and capacity to undertake the responsibility for ongoing monitoring of the fulfilment of AML/CFT duties by the institution (including sample testing of compliance, reviewing exception reports and being the contact point regarding all AML/CFT issues for internal and external authorities including supervisory authorities or the FIU/FID)[214] and

(d) is independent of the business lines of the institution to allow for an objective assessment and monitoring and enforcement of the compliance of the institution's operations and decision making with its AML/CFT obligations under the country's framework and with the institution's own AML/CFT policies and procedures. Basel's recommendation is that regardless of the institution's size or its management structure, potential conflicts of interest should be avoided. Therefore, to enable unbiased judgments and to facilitate impartial advice to management, the chief AML/CFT officer should, for example, not have business line responsibilities and should not be entrusted with responsibilities in the context of data protection or the function of internal audit[215]. The Basel's recommendation also reflects that where any conflicts between business lines and the responsibilities of the Chief AML/CFT officer arise, procedures should be in place to ensure AML/CFT concerns are objectively considered at the highest level.

[213] Basel Committee on Banking Supervision – Sound management of risks related to ML and FT, January 2014 (Assessment, understanding management and mitigation of risks – page 5)

[214] Ibid, The Basel Committee on Banking Supervision also reflects the chief AML/CFT officer should also have responsibility for reporting suspicious transactions.

[215] Ibid

234. The nominated officer is responsible for reporting to the Designated Authority[216], all such activities as required by the relevant statutes and the Guidance Notes, and should be in a position to provide advice and guidance to the staff of that institution, on the identification of suspicious transactions (See Appendix IV - List of Duties and Responsibilities of the Nominated Officer'). In providing such advice and guidance the nominated officer should pay attention to any advisories or guidance that may be issued by the designated authority in relation to reporting obligations under the AML/CFT laws and should consult with the designated authority accordingly.

228. An institution's policy manual should require the preparation and submission of reports by the Nominated Officer to the Board of Directors (or such other governing body by whatever name called which performs such functions) at least once a year or at more frequent intervals as warranted by the risk profile of the financial institution and which ensures the board is at all times fully aware of the ML and FT risks faced by the institution and of the effectiveness of the institution's measures to address these risks. This report should, at a minimum include:-

(a) an overview and evaluation of the overall effectiveness of the institution's AML/CFT framework, the effectiveness of AML/CFT measures implemented under each of the various operational areas and/or product and service types as well as AML/CFT training exercises completed (training exercises should extend to training regarding compliance with directives to apply targeted financial sanctions notified by the United Nations Security Council) and initiatives pursued for that licensee's financial year.

(b) The licensee's compliance with relevant legislation and BOJ's Guidance Notes and guidance issued by the designated authority in relation to the institution's AML/CFT reporting obligations, reporting obligations pertaining to compliance with directives to apply targeted financial sanctions as notified by the United Nations Security Council as well as the licensee's own policies and procedures and the programmes and policies for the financial group (where applicable);

(c) particulars of the risk assessment and risk management activities (see Section IV above) including:-

[216] POCA section 95; TPA section 18(3);

(i) Report on the adequacy and effectiveness of the licensee's risk assessment processes;

(ii) Detailed assessment of effectiveness of monitoring of high-risk customers and information as to any challenges posed by that area of the licensee's operations;

(iii) Report on the financial institution's level of compliance in updating its customer records for pre-existing customers; and in obtaining the approval of senior management for transacting business with, or involving products, services, customers of jurisdictions assessed as posing a high risk of ML or TF to the financial institution;

(iv) Continued relevance of measures employed to mitigate, minimise or otherwise manage risks identified;

(d) Number and frequency of threshold reports, required disclosures (suspicious transactions/activities) detected and other reportable matters reported to the designated authority;

(e) Any significant and/or unusual trends in evidence arising from a review of transactions detected and reported (e.g. trends in relation to specific branches, geographic areas – local and/or overseas, or types of transactions; customer profiles etc.);

(f) Report on the financial institution's compliance in relation to customer due diligence and know your customer standards as set out in these Guidance Notes as well as in the financial institution's own policy;

(g) Report on the findings of the annual and any other intervening AML/CFT audits undertaken by the institution's external and internal auditors, and findings emanating from reviews by BOJ examiners; as well as steps taken to effectively address AML/CFT weaknesses or deficiencies detected or identified;

(h) Update on programmes employed over the reporting period for targeting employee awareness and integrity - including training programmes for the Board (or other

governing body by whatever name called) executives, senior management, staff (and wider application as deemed appropriate) and the effectiveness of such programmes;

(i) Update on the financial institution's overall relationship with the Designated Authority and general guidance received from that body;

(j) Advice on any proposed/impending legislative/regulatory changes as regards AML/CFT, with an assessment of how the institution will be impacted and advice as to how necessary operational changes will be implemented to ensure continuing adherence by the financial institution.

236. This report must be readily available to or accessible by the BOJ. Financial institutions will note that the current AML/CFT examinations include and will continue to include specific checks to ensure compliance with AML/CFT training requirements for employees.

SECTION VII – COMPLIANCE MONITORING

INTERNAL COMPLIANCE PROGRAMME

237. An effective internal compliance programme is essential to a financial institution's endeavour to comply with its obligations under the law, prevent involvement in illicit activities and adhere to international standards.

238. The POCA and the TPA specifically require that financial institutions make arrangements for an independent audit, in order to ensure that the statutory requirements and the programmes itemized in these Guidance Notes and adopted in policy manuals, are being implemented. An officer at the senior management level must have explicit and ultimate responsibility for the financial institution's internal compliance program (Refer to Section VI above), which at a minimum would involve: -

(a) Establishment of an adequately resourced unit responsible for day to day consideration and monitoring of compliance;

(b) Establishment of a strong compliance plan that is approved by the Board of Directors of the institution and that provides for ongoing independent review and testing of staff's compliance with AML and CFT requirements;

(c) Proactive follow-up of exceptions to ensure that timely corrective actions are taken;

(d) Regular reporting of compliance levels, including exception reporting to senior management. Senior management should also be made aware of any corrective measures being implemented;

(e) Regular consultation with the Designated Authority to ensure that the institution is carrying out its obligations under the law.

(f) Regular or periodic reviews of the AML/CFT program including (the Compliance Unit) by the internal and external audit functions. The timing of these reviews should be informed by, among other things, the institution's risk profile.

239. Each financial institution shall:-

(a) establish clearly defined policies and operational procedures in regard to the matters at paragraphs 102 and 103 above;

(b) ensure that AML/CFT policies and procedures are informed by the financial institution's assessment of its risks as discussed in Section IV above.

(c) ensure that the AML/CFT policies and procedures are:-

(i) properly documented in the form of a manual for distribution among, or which is readily available to all relevant staff. The distribution process may be evidenced by the employee's signing in confirmation that the manual has been received or accessed or alternative process which is equally effective;

(ii) ensure that this manual is reviewed at least on an annual basis and make appropriate revisions and enhancements when necessary;

(iii) ensure that the manual and all subsequent revisions thereto are reviewed and approved by the Board.

Non-compliance with these requirements will amount to a breach of the AML/CFT Supervisory Rules.

240. A financial institution shall ensure that the policies and programmes contained in its manual include the following:

(a) measures and procedures which are commensurate to the risks that have been identified from the institution's assessment of its risks;

(b) the establishment of procedures to ensure high standards of integrity for employees at all levels including senior and executive management levels;

(c) the development of a system to evaluate the personal employment history and financial history of all employees at all levels including senior and executive management levels. Financial institutions are expected to establish specific procedures for such evaluation at the point of hiring, although ongoing evaluation would also be expected throughout the period of employment;

(d) the establishment of programmes for the training of employees on a continuing basis, and for instructing all employees as to their responsibilities in respect of the law, regulatory guidance and 'best practice' standards; (In considering the impact of the regime in this regard, financial institutions must bear in mind the defences that can be raised by a person charged with any of the foregoing offences. For example under POCA, not only can a person raise the defence that he or she did not know or suspect that another is engaging in money laundering, he/she can also claim that the requisite training was not provided to him or her by the employer. The defence appears to require proof of both elements (i.e. lack of knowledge/suspicion and lack of training) in order to be successfully raised.[217]

[217] Section 94(6), POCA

(e) the establishment of comprehensive customer due diligence policies and procedures, incorporating adequate customer acceptance policies and a multi-tiered customer identification programme that involves more extensive and rigorous due diligence to allow for adequate identification of ultimate beneficial owners; and are applied to high risk customers/accounts, as well as transactions with non- face-to-face and overseas customers and counter-parties;

(f) designation of an officer of the institution at the senior management level to be the institution's Nominated Officer, responsible for ensuring the effective implementation of the policies, programmes, procedures and controls including reporting to the appropriate authorities, of threshold and suspicious transactions and asset holdings re: listed entities or entities designated in relation to the UNSEC resolutions regarding the prevention of the proliferation of weapons of mass destruction;

(g) full co-operation and consultation with the relevant authorities, primarily the Designated Authority and the Competent Authority, for the purpose of carrying out the institution's obligations under law and best practice standards;

(h) procedures for analysis of clients' transactions to ascertain trends and to recognize indicators of unusual and/or suspicious activity over time, e.g. multiple small transactions aggregating to a specified limit in a month, or annually;

(i) procedures for analysis of transactions (other than customer related transactions) that are undertaken in the course of business to determine whether the transaction is one in relation to which a required disclosure should be made. Examples of such transactions would include the following:

(i) correspondent banking arrangements (both within the island and cross border);

(ii) proprietary transactions such as securities transactions;

(iii)fixed asset acquisitions and disposals; and

(iv) custody arrangements

(j) arrangements for regular and timely internal and external audit reviews in order to ensure that there is adherence to the documented policy and procedures;

(k) provision for the heightened scrutiny of certain categories of customers and types of transactions when necessary, as well as the continuous review of existing practices and procedures in this area as part of the general internal/external audit and control processes.

Non-compliance with these requirements will amount to a breach of the AML/CFT Supervisory Rules.

241. The procedures discussed at paragraphs 239 - 240 must include measures for:

(a) customer (including beneficial ownership) identification and verification **prior** to the commencement of business relationships and on an ongoing basis thereafter, using reliable independent source documents, data or information;

(b) taking reasonable measures to establish the source of the customer's wealth as well as the source of funds involved in the transaction and transaction verification in respect of customer and other transactions prior to the commencement of the commercial arrangement, business relationship or transaction.

(c) documenting and maintaining records of transactions[218];

(d) recognizing and recording suspicious transactions as well as threshold transactions and applicable property under the TPA or freezable assets under the UNSEC Implementation Act and establishing clear procedures for ensuring the required reports are made in relation to these matters;

(e) ensuring compliance with relevant legislation, and co-operation with enforcement authorities;

[218] POC (MLP) Regulations, r. 14(4)

(f) internal audit checks to ensure compliance with policies and procedures relating to money laundering and terrorist financing;

(g) the training of staff in the operation and implementation of procedures and controls relating to the combatting of money laundering, terrorist financing, the prevention of the proliferation of weapons of mass destruction activities and their obligations under the law;

(h) communication of group policies and procedures on the detection and prevention of money laundering, terrorist financing, and the proliferation of weapons of mass destruction activities and the monitoring of compliance by all subsidiaries and branches whether located in Jamaica or overseas.

242. A financial institution shall adopt a consolidated approach to the establishment and implementation of its AML/CFT policies and procedures, which shall cover the activities of all local and foreign branches, subsidiaries[219]. In this regard financial institutions should note the relevant sections of these Guidance Notes regarding the obligations for financial holding companies, and responsibilities in respect of branches and subsidiaries.

SECTION VIII - BOARD RESPONSIBILITY & EMPLOYEE INTEGRITY AND AWARENESS

BOARD RESPONSIBILITY

243. The board of directors of a financial institution must have a clear understanding of the ML/TF risks faced by the financial institution[220]. This includes a good working

[219] FATF Recommendation 18

[220] Basel Committee on Banking Supervision – Sound management of risks related to ML and FT, January 2014 – wwww.bis.org.

knowledge of the operating risks faced by the institution (i.e. based on the services and products offered; customer base; strength of internal controls and hiring policies). The board must also be actively aware of risks posed to the financial institution where it resides within a financial group or within a broader corporate structure as well as the broader risks posed to the financial institution from a national perspective. Risks from the national perspective include broader concerns – performance of the economy; levels of crime and types of crimes to which financial services are most vulnerable; the country's external ratings in the areas of- credit risk; transparency; cooperation; and inclusion in watch lists, or lists which require other countries to apply certain economic measures (including financial sanctions) before or when undertaking dealings with the country.

(a) The board of a financial institution must therefore be satisfied that:-

(i) the institution's risk assessment accurately and appropriately reflects the ML and TF risks faced by the institution and accurately reflects the effectiveness of the institution's measures to address these risks, and is updated to ensure that this objective is met on an ongoing basis;

(ii) the officer who is appointed to carry out the function of the nominated officer is appropriately qualified, and has the requisite stature and authority to undertake the responsibilities of that function and to effectively execute that function[221] (refer to Section VI). In this case 'authority' means, sufficient authority within the financial institution such that issues raised by this officer receive the necessary attention from the board, senior management and business lines;

(iii) that the reports by the nominated officer are provided in a frequency that accords with the risk profile of the financial institution and ensures the board is at all times fully aware of the ML and FT risks faced by the institution and of the effectiveness of the institution's measures to address these risks; and

[221] Ibid

(iv) that the institution has adequate policies and processes for screening prospective and existing staff or employees to ensure high ethical and professional standards.

(b) the board must ensure that the institution's AML/CFT policies and procedures are effectively implemented. This means -

(i) implementation in a manner which accords with functional implications, i.e. areas comprising front line functions; high levels of interaction with the public; sensitive functions (such as cash transactions; cash management functions; treasury functions; preparation of accounts; data input and analysis); compliance and oversight functions should be subject to the more intensive and most frequent levels of AML/CFT training and information;

(ii) ensuring the internal audit function assesses the risk management practices and internal controls of the institution including periodically assessing the effectiveness of the institution's compliance with its AML/CFT policies and procedures;

(iii) compliance and oversight functions are provided with adequate or sufficient resources to ensure that AML/CFT policies and procedures are effectively implemented and

(iv) ensuring the external audit function engagement extends to the institution's compliance with its AML/CFT policies and procedures.

(c) the board must ensure it receives adequate and appropriate exposure to training materials and updates on the local AML/CFT laws and framework as well as the

international standards and best or sound practices which impact AML/CFT obligations for financial institutions.

EMPLOYEE INTEGRITY AND AWARENESS

244. Financial institutions need to be cognizant of the risks attached in having inadequate hiring policies and in having inadequate systems to deal with for instance dishonest employees since the success of an institution's AML/ CFT programme depends to a large extent on the integrity of its employees. Additionally, financial institutions are mandated to establish and implement appropriate policies and procedures[222] to ensure that (where applicable and as far as possible) employees are "fit and proper" persons.

Tolerating the continued rotation of unscrupulous or dishonest employees within the financial system exposes financial institutions to AML/CFT risks and to increased possibilities of AML/CFT breaches. As such unscrupulous or dishonest employees should be subject to the appropriate disciplinary action and prosecution, where the circumstances warrant this. Such persons should not be permitted to move through the financial system due to the insufficient disclosure or the absence of full and frank disclosure of the activities of such employees. (A classic example of this is an employee who has been found to be colluding with customers to commit frauds against the financial institution and who, instead of being fired and prosecuted, is given the option of resigning quietly, leaving this person to continue to seek employment within the financial system with another unsuspecting financial institution. In some cases, employer references are still provided in relation to such persons.) This will no doubt remain an issue that must be balanced against the hazards of lawsuits by such employees and as such financial institutions will need to work closely with their legal advisors on how such matters should be addressed.

[222] POC (MLP) Regulations, r. 5; TPA section 18.

Know Your Employee

245. Potential candidates for employment should be subject to a comprehensive screening process, which should involve a thorough investigation of that candidate's background (including employment and financial history (including credit history), and criminal background), honesty, competence and integrity.

(a) In relation to staff or employees, financial institutions are expected to have in place the requisite policies and procedures that permit or facilitate or allow ongoing monitoring of an employee's-

(i) Competence to undertake the role or position to which the employee is assigned;

(ii) Legal compliance with the statutory obligations that may apply to the employee specifically (such as income tax requirements; professional standards and requirements; obligations under the corruption laws;

(iii) General character (eg. tendencies to commit offences – minor and substantial)

(iv) General compliance with the institution's policies and procedures;

(v) Adherence with ethical practices and conduct;

(vi) Behaviours exhibited which accord with ethical and moral standards – (behaviours in this category generally include:

1. Ability to be forthright;
2. Absence of or prompt declaration of conflict of interest issues;
3. Culture of loophole mining –whether with internal policies or in relation to the institution's statutory obligations;
4. Culture of compliance – with internal policies and with the institution's statutory obligations;
5. Tendency or propensity to lie, cheat, mishandle the institution's property – including borrowing without permission, stealing, handling the property so recklessly or negligently – whether or not this results in damage to the property.

246. Financial institutions must also institute processes geared towards ensuring the continued maintenance of a high level of integrity and competence among staff. These may include: -

(a) Establishment of a Code of Ethics to guide employee conduct;

(b) Establishment of a 'whistle blower' policy;

(c) Regular review of employee's performance and adherence to internal policies and procedures including codes of conduct and AML/CFT requirements;

(d) Imposition of appropriate disciplinary actions for breaches of the institution's AML and CFT policies and procedures;

(e) Imposition of appropriate disciplinary actions or taking other appropriate where an employee is convicted for committing an offence that involves dishonesty or for committing an offence which can result in a designation of criminal lifestyle being applied in accordance with section 5 of the POCA; and

(f) Close scrutiny and investigation of employees whose lifestyles cannot be supported by his or her known income.

EDUCATION AND TRAINING[223]

247. In order to ensure full implementation of the procedures, recommendations, and requirements contained in these Guidance Notes, the staff/employees of financial institutions must be made fully aware of the serious nature of money laundering crimes and terrorism financing activities. Furthermore, efforts must be made to ensure that all staff or employees understand the basic provisions of the POCA, the POC (MLP) Regulations, the TPA and the TP (Reporting Entities) Regulations.

248. Members of staff must also be sensitised as to their personal obligations under the POCA and the TPA and the fact that they can be held personally liable for failing to report relevant information to the Designated Authority (in the case of nominated officers), or otherwise failing to carry out their responsibilities under the relevant statutes.

[223] See POCA (MLP) Regulations MLA section 7(2)(c)

249. In considering the impact of the regime in this regard, financial institutions must bear in mind the defences that can be raised by a person charged with any of the foregoing offences. Under the POCA, not only can a person raise the defence that he or she did not know or suspect that another is engaging in money laundering, he/she can also claim that the requisite training was not provided to him or her by the employer[224]. The defence appears to require proof of both elements (i.e. lack of knowledge/suspicion and lack of training) in order to be successfully raised. Under the TPA a defence of having a reasonable excuse for not making a report (re: assets held for listed entities or STRs) can be raised in relation to proceedings for an offence under section 15 or section 16). The term 'reasonable excuse'[225] is not defined in the TPA. Additionally, a staff member (other than the nominated officer, who is charged with an offence of not making a report under section 16, can raise the defence that the information or other matter, was disclosed to the nominated officer in accordance with the procedures established pursuant to section 18 of the TPA.

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

(a) Employment;

(b) Promotion/lateral movement to sensitive or frontline duties;

(c) Expiration of minimum period since last training session which triggers refresher requirements;

251. Training initiatives can either be confined to scheduled sessions or expanded to include spontaneous spot checks within randomly selected areas of operation both in-house (i.e. via Department; or via frontline staff operations; or via sensitive operations) or randomly selected branches and subsidiaries. A mixture of such processes is likely to result in a more robust system that can quickly reveal shortfalls for the managements' attention as against relying on a system that is confined to scheduled, standard one style of training

[224] See the POCA section 94(6)

[225] Stroud's Judicial Dictionary of Words and Phrases – discusses the meaning of the term 'reasonable excuse' with case law speaking to the meaning of the term – in a number of circumstances including ignorance of a requirement to act; honestly and reasonably believing the activity does not amount to a prohibited activity; failure to comply with a requirement on the basis of fear of self-incrimination. (8th edn. Volume 3)

method which is less likely to readily reflect shortfalls and areas of weakness that can be quickly addressed.

252. Financial institutions must ensure that satisfactory steps are taken to confirm/prove that training of employees took place. Such steps may include, but are not limited to the following:-

(a) Ensuring such sessions are subject to rigorous registration systems that require signing by trainees and or trainers and true records of the training session documented and retained in formal training registers; and /or

(b) Videotaping of scheduled training sessions (best used in seminar type training scenarios. In that regard, seminar participants must be aware that the session is being taped or recorded in any way; and

(c) Delivery of documented certifications to employees evidencing satisfactory completion of training session; and

(d) Separate verification of the training sessions having taken place by the nominated officer; and/or

(e) Sign off on the sessions taking place by the Board of the financial institution as a part of the audited annual report of the financial institution.

253. Financial institutions must therefore introduce programmes to ensure that staff or employees**,** are informed of their responsibilities, and encouraged to provide prompt notification of suspicious as well as threshold transactions. The timing and content of training for staff or employees should cover all critical areas of operation from senior management through to 'rank and file' and be tailored according to the risk profile of the institution, job functions and responsibilities and the risk factors to which employees are exposed due to their functions and responsibilities. This means ensuring ease of access

to the requisite policies and manuals is afforded to staff or employees at all levels by for instance:-

(a) ensuring such documents are available on internal electronic access (eg. intranets);

(b) ensuring sufficient copies are placed in resource centres or libraries in-house; and

(c) ensuring the timely circulation of updates and amendments throughout the institution network (i.e. head office to branches and representative offices and parent companies to subsidiaries.)

254. Training/education programmes must be designed and implemented on an ongoing basis by individual institutions to ensure employees' awareness of: -

(a) Current as well as new and developing AML and CFT laws, regulations, standards and guidelines being established both locally and internationally;

(b) Their legal obligations and responsibilities to prevent and detect money laundering and terrorism financing;

(c) New money laundering and terrorism financing techniques, methods, typologies and trends;

(d) The institution's own AML and CFT policies and procedures.

255. In developing education and training programmes[226], particular emphasis needs to be placed on the following categories of staff:

(a) **New Employees/Staff.** All new employees/staff, irrespective of their level of seniority, should be informed as to the background and nature of money laundering and terrorist financing and the need for reporting suspicious and threshold transactions to the Designated Authority, through the institution's Compliance Officer. They should be made aware of their personal legal obligation as well as that of the institution, to report suspicious transactions. As mentioned above, institutions should also institute appropriate screening processes so as to thoroughly investigate the background, honesty, and integrity of prospective employees.

[226] Interpretive Note to FATF Recommendation 18

(b) **Front Line Staff/Employees**. The first point of contact of an institution with potential money launderers or persons attempting to finance terrorist activities is usually through staff/employees who deal directly with the public. 'Front-line' staff members/employees (such as Tellers, Cashiers and Foreign Currency Staff, and Receptionists) should therefore be provided with specific training on examples of suspicious transactions and how these may be identified. They must also be informed about their legal responsibilities and the institution's reporting systems and procedures to be adopted when a transaction is deemed to be suspicious. Additionally, they must be informed as to the institution's policy for dealing with occasional customers and 'one off' transactions, particularly where large cash transactions are involved.

(c) **Account Opening/Customer Service Staff/Employees**. Members of staff/employees who deal with account opening, or the approval of new customers must receive the training given to tellers etc. in (b) above. They should also be trained as to the need to verify the identity of a customer and the institution's account opening and customer verification procedures. They must further be advised that a business relationship or 'one-off' transaction should not be established or continued until the identity of the customer is verified. Staff or employees should also be made aware that the offer of suspicious funds or the request to undertake a suspicious transaction should be reported to the Nominated Officer, whether the funds are accepted or not, or the transaction proceeded with, or terminated.

(d) **Administration/Operations Supervisors and Managers**. A higher level of instruction covering all aspects of AML/CFT procedures should be provided to persons with the responsibility for supervising or managing staff. Such training must include familiarization with the offences and penalties arising under the POCA and the TPA, the procedures relating to monitoring orders and production orders, the requirements for non-disclosure and for retention of records, and management's

specific responsibility vis `a vis dealings with customers in accordance with the risk profiles applicable to those customers.

SECTION IX - TRANSACTION MONITORING & REPORTING

REQUIRED DISCLOSURES - RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS & FINDINGS IN RELATION TO UNUSUAL TRANSACTIONS

256. A suspicious transaction will often be inconsistent with a customer's known legitimate business or personal activities or with the normal business for that type of account or with the nature of the transaction indicated. Hence, general knowledge of the nature of the industry or sector in which the customer operates and the nature and pattern of the customer's own business, and a good understanding of the operating environment and the banking processes that would be applicable to the various services and products offered are the first set of elements in recognizing a suspicious transaction or an unusual transaction or series of transactions.

257. Section 94(3) of the POC (Amendment) Act states that a required disclosure is a disclosure of information or other matter on which the knowledge or belief is based or which gives reasonable grounds for the knowledge or belief that another person has engaged in a transaction that could constitute or be related to money laundering, made to either the nominated officer or to the designated authority. Under the TPA the suspicious transaction reporting obligation is stated a little differently, it refers to each entity reporting to the designated authority, all transactions, whether completed or not, which the entity suspects, or has reasonable cause to suspect involves property connected with

or intended to be used with the commission of a terrorism offence or involve, or are for the benefit of, any listed entity or terrorist group. Reporting to the designated authority is subject to use of a statutory form[227] .

258. The law reflects that a required disclosure under the POCA or the TPA is one that should be made to the nominated officer or designated officer[228]. In practice, and for good order reports of regulated businesses should be made to the designated authority through the nominated officer who will thereafter be required to make a disclosure in the statutory form to the designated authority; and

259. In complying with the obligation to report suspicious transactions under the POCA and the TPA, a financial institution is also required to:-

(a) pay attention[229] to (or identify and take notice of) -

(i) complex, unusual or large business transactions or unusual large transactions carried out by the customer with the financial institution; and

(ii) unusual patterns of transactions.

(b) make a record of the transactions at (a) and the related findings[230];

(c) where the circumstances occur in relation to s. 16(3) of the TPA ensure that the findings and transactions are made available, on request, to its auditors and to the designated authority[231]; The POCA does not expressly require findings and transactions to be treated in the same manner as under the TPA, however, for good practice and order, it is recommended that this category be made available on request to auditors, a supervisory authority or the competent authority and reported to the designated authority under POCA.

[227] Regulation 17(2) of the TP (Reporting Entities) Regulations, 2010
[228] POCA section 94(3); TPA section 18(3) re: a section 16(3) report (unusual transactions) & section 16(3A) re: a STR)
[229] Section 94(4)(a) POCA; section 16(3)(a) TPA.
[230] Section 94(4)(a) POCA; section 16(3)(b) TPA
[231] Section 94(4)(b) POCA (but only in relation to transactions involving customers in territories listed in accordance with this section. in this case findings should be available on request to a supervisory authority or competent authority concerned. Auditors are not mentioned in the POCA); section 16(3)(b) of the TP(Amendment) Act, 2011.

(d) pay special attention to all business relationships and transactions with any customer resident or domiciled in a territory specified in a list of applicable territories published by notice in the Gazette by a supervisory authority for the purposes of section 94(4)(b) of the POC (Amendment) Act, 2013 and ensure that the findings are available upon request to the designated authority, s supervisory authority or the competent authority.

260. When a financial institution is faced with a situation or circumstances in respect of which it would be reasonable for a required disclosure (i.e. STR) to be made, that institution must either –

(a) refuse to conduct the transaction; refuse to commence the relationship or decline from undertaking any business arrangements in respect of the customer or transaction or arrangement that is deemed suspicious; or

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

261. Severe implications can arise from a financial institution being viewed as one that is holding property or providing financial services to facilitate money laundering or the financing of terrorism (such as prosecution; reputation risk, loss of correspondent banking relationships). Accordingly, a financial institution shall ensure that reports made to the Designated Authority by the institution are followed up by specifically assigned senior officers (i.e. the nominated officer himself/herself or his/her highly ranked designate) such that at anytime an institution is called on, it is in a position to provide more information than merely that "the matter was reported to the Designated Authority". The institution shall also ensure that the account or transaction is followed up and regularly analyzed and it must be clear from the records of the institution the point at

which a determination was made to apply appropriate counter measures to safeguard the institution. Countermeasures include action to:

(a) close the account;
(b) end the business relationship;
(c) terminate the transaction;
(d) scale down services;
(e) refuse to undertake transactions above or under a certain amount;
(f) refuse to undertake new business with the customer;
(g) refuse to accept introduced business from that customer or in relation to that customer.

A failure to comply with this requirement will amount to a breach of the AML/CFT Supervisory Rules.

262. The application of appropriate countermeasures by a financial institution will be indicative of a financial institution acting to protect itself and the integrity of the overall financial system. Such steps may ultimately be the determining factor in whether an institution is viewed as "complicit" in its dealings generally or with the customer; and whether it is negligent or is recklessly aiding and abetting the customer/(s) in question. In complying with their obligations under the POCA or the TPA (whichever is applicable) in this regard, financial institutions should consult closely with their respective legal advisors.

263. Financial Institutions should also note the following-

(a) if the institution is placed in a position where it is of the view that it must proceed with the transaction, relationship or arrangement, **and** in the institution's view the circumstances do not permit the institution to make the relevant disclosure and secure the appropriate consent before proceeding then the institution must ensure that the

relevant disclosure is made on its own initiative and as soon as is reasonably practical for this to be done. (section 100(4) &(5))[232];

(b) acting in accordance with (a) does not necessarily absolve the institution from making the requisite disclosure or obtaining the appropriate consent, in relation to the continued offering of any service or facility or in transacting further business in relation to the customer or the property in respect of which the knowledge or belief that criminal activity is taking place was formed. For the avoidance of all doubt, institutions must actively seek the necessary guidance, directive or consent from the designated authority before proceeding in any manner.

A financial institution must therefore satisfy itself that the direction or consent obtained from the designated authority **clearly permits or prohibits** the doing or undertaking of any activity in relation to accounts, transactions, customers or property in respect of which authorized disclosures have been made.

264. Financial institutions should have adequate systems in place to ensure the timely, ongoing detection and reporting of complex or unusual large transactions, holdings of property owned or controlled by a listed entity, suspicious and threshold transactions and bring these to the attention of the relevant authorities.

(a) The requirement to '*pay attention to*" or *"pay special attention to"* to certain transactions as used in the POCA section 94(4)(b) and as used in section 16 (3) of the TPA includes not only identifying and taking notice of the types of transactions described in these sections of the law but also the examination of the background and purpose of these types of transactions, the formal recording of the institution's findings and the retention of these findings for a period not less than 7 years.

(b) Financial Institutions must also be in a position to make their findings in this regard available to BOJ, whether during on-site examinations which includes an assessment of

[232] A similar provision is also found at section 93(2), which from the general wording appears applicable generally to persons other than a person who is a business in the regulated sector.

the institutions' AML/CFT systems or otherwise on request. These findings must also be available to the designated authority[233].

(c) Financial institutions are reminded that not only is an institution's failure or inability to comply with its statutory reporting obligations, an offence under POCA and the TPA, such failures can also constitute behaviour in respect of which remedial action can be directed or imposed on institutions under their respective governing statutes, for instance by the Supervisor pursuant to section 109 of the BSA. Additionally, under paragraph 2 of Part A to the Fifth Schedule to the BSA, an institution which is a licensee under the BSA can also be deemed to be engaging in unsafe or unsound practices. Any deficiencies in the systems, which place the institution in breach of its obligations under the governing statutes may also be reported to the Designated Authority.

(d) The POCA is silent on the matter of the availability of an institution's records pertaining to documented findings being available to its external auditors. An institution may be guided by section 97(2)(b) of the POCA which outlines disclosures made under certain circumstances, which would not be deemed as "tipping off". Subsection (b) specifically speaks to circumstances where the disclosure is made in carrying out a function the person has relating to the enforcement of <u>any</u> provision of the POCA or of any other enactment relating to criminal conduct or benefit from criminal conduct. A financial institution would however be expected to exercise discretion and judgement to ensure that in-house disclosures to internal auditors and disclosures to external auditors[234] occur only to the extent and in a manner that will allow those critical functions to carry out their obligations under POCA and its Regulations. <u>In addressing this issue financial institutions should consult closely with their respective legal advisors.</u>

265. There are certain categories of activities that are suspicious by their very nature, and should alert a financial institution as to the possibility that a customer is seeking to conduct illegal activities at/through the institution. Examples of such suspicious conduct

[233] Section 94(4)(b) - POCA
[234] POC (MLP) Regulation 5(2)(d); TPA section 18(2)(d)

and activities are outlined in Appendix V. This listing is not intended to be exhaustive, and only provides examples of the most basic ways by which money may be laundered and forms the catalyst for prompting enquiries about the source of funds and source of wealth and for applying enhanced due diligence measures. Financial institutions should also keep themselves informed as to the constantly evolving methods (i.e. typologies) of money laundering and terrorist financing. Financial institutions should note that under the POCA any offence in Jamaica can constitute a *predicate offence*. This is an expansion of the category under the repealed Money Laundering Act of offences in respect of which a charge of money laundering could be laid. Therefore required disclosures (STRs) should be made in cases where there is suspicion that the transaction being conducted is facilitating theft of funds; funds received through for instance insider trading activities; funds diverted to evade the payment of taxes or to otherwise deprive the Government of revenues; funds comprising bribes or diversion of public funds and so forth.

266. Financial institutions should have adequate systems in place to ensure the timely, ongoing detection and reporting of suspicious and threshold transactions, and holdings of property owned or controlled by a listed entity and to ensure timely identification of complex or unusually large transactions.

267. The reception point for disclosures under the POCA and the TPA (whether these are suspicion-based reports or reports of transactions at or above threshold limits or reports re: asset holdings) is the Designated Authority. Financial institutions also need to ensure that the requisite statutory reporting forms are properly completed to facilitate the investigatory process that may be undertaken as a consequence of the report and to ensure compliance with reporting obligations is achieved.

268. Financial institutions should establish systems that ensure all matters identified for reporting under the TPA or POCA are brought to the attention of the Nominated Officer. Each case must then be reviewed at that level to determine whether the suspicion is justified, and in the absence of factual information to negate the suspicion, the Nominated Officer should expeditiously submit a report to the Designated Authority, within the

stipulated statutory period. In this regard it should be noted that both the POCA and TPA speak to making the required disclosure or report "*as soon as is reasonably practicable and in any event within 15 days*[235]*."* The specific steps that must be followed for the reporting of such transactions must be clearly outlined in the policy manual and communicated to all relevant personnel. The following must also be noted: -

(a) Both the POCA (MLP) Regulations and TP Reporting Entities Regulations, provide for the use of a standard reporting format[236], which must be adopted.

(b) The POCA has established the following **reporting and feedback regime for required disclosures**.

(i) Where circumstances in which a required disclosure should be made arise then in the case of persons operating in a regulated business (eg. financial institutions) the matter must be brought to the attention of the Nominated Officer within 15 days of the incident occurring (i.e. the suspicious transaction; and/or the realization being formed that the transaction is suspicious).

(ii) After assessment/analysis of the matter with the institution's Nominated Officer, if the determination made is that the matter qualifies as one in which a required disclosure should be made then the Nominated Officer must make the required disclosure within fifteen days after the information or matter comes to that officer's attention.

(iii) The required disclosure takes place in the form prescribed by the POCA (MLP) Regulations and is made to the Designated Authority.

(iv) The financial institution's treatment of the matter subsequent to the required disclosure being made must be in accordance with the statutory feedback regime termed **"appropriate consent"** which can be found under sections 91 and 99 of the POCA.

[235] POCA section 94(2)(c); and the TPA section 16(3A)
[236] POCA (MLP) Regulations, 2007 Schedule to r. 17 Forms I and II; and TP (Reporting Entities) Regulations, 2010 Schedule to regulation 17 Forms 1 and 2

Appropriate consent regime

269. In the case of financial institutions-"appropriate consent" exists

(a) After the Nominated Officer makes a disclosure to the Designated Authority, and that Officer has received a response from the Designated Authority within seven days (exclusive of weekends & public holidays and starting the day after the disclosure is made), consenting to the Nominated Officer undertaking a prohibited act; (s.99(1)(a))

(b) After the Nominated Officer makes a disclosure to the Designated Authority, and that Officer has **not** received notification from the Designated Authority within the seven days' notice period prohibiting the Nominated Officer from undertaking a prohibited act; (s. 91(2)(b)(i) and 99)(1)(b);

(c) After the Nominated Officer makes a disclosure to the Designated Authority, and that Officer has received notification from the Designated Authority within the seven days' notice period prohibiting the Nominated Officer from undertaking a prohibited act but ten days have passed since the receipt of that notice; (s. 91(2)(b)(ii) an 99(1)(c). It should be noted that the relevance of this ten day period is used to ensure that if by the expiration of that period no further action has been taken by the relevant authorities in relation to the matter disclosed, the financial institution is deemed to have attained the status of "having the appropriate consent" to undertake the prohibited act. Further action would include steps such as obtaining a court order restraining the financial institution from dealing with the property in question.[237]

(d) The POCA provides for the consent or refusal of consent by the Designated Authority to be verbally communicated to the reporting regulated business, however this must be followed up within five days by the written notification. (S. 99(4))

(e) If the institution is placed in a position where it is of the view that it must proceed with the transaction, relationship or arrangement, **and** in the institution's view the

[237] K. Ltd. v. National Westminister Bank plc. [2006] EWCA Civ. 1039 70KB All ER.(D) 131 (Jul)

circumstances do not permit the institution to make the relevant disclosure and secure the appropriate consent before proceeding, then the institution **must** ensure that the **relevant disclosure is made on its own initiative** and **as soon as is reasonably practical** for this to be done. (section 93(2); 99(1&2) and 100(4) & (5))

270. The reporting and feedback regime for required disclosures established under the POCA are not in place under the TPA. It is therefore expected that in so far as business efficiency is concerned and the practicalities and legality of the situation permits, financial institutions may consider implementing a similar reporting and feedback regime for matters arising under the TPA framework in consultation with the designated authority. However, financial institutions must bear the following in mind –

(a) The concept of appropriate consent is not statutorily established under the TPA as such the statutory indemnities that accompany that regime will not be applicable. This may be because in so far as situations that may be the subject of an STR involving a listed entity pursuant to an Al Qaeda or Taliban UN Resolution, consent to do business with that entity cannot be allowed outside of a process that involves the court (eg. the circumstances outlined in the TPA framework treating with the matter of reasonable living expenses of a person or reasonable business or legal expenses of a person impacted by a restraint order as described under section 42(1)(a) and 42(5)(c); or section 31 of the TPA regarding the protection of the interests of third parties).

Comment [CM9]: Specific comment on this further discussion is invited.

(b) STRs arising under the TPA framework must be reported to the designated authority within 15 days. (Under the POCA framework there is a maximum 30 days window within which a regulated business must report a suspicious transaction to the designated authority - i.e. for the discovering officer to report the matter giving rise to the suspicion to the Nominated officer within 15 days of the matter that is the cause of the suspicion; and then the Nominated officer has to report the matter to the designated authority within 15 days of the matter coming to his attention.)

271. Onward disclosures pertaining to suspicious transaction reports made, or investigations (whether pending or ongoing), under the POCA or under the TPA will not amount to an offence if[238]-

The circumstances of disclosure	POCA/TPA	Section
At the time of the disclosure the person did not know or suspect that the disclosure would be prejudicial to any investigations under the Act;	POCA	97(2)(a)
The disclosure is made pursuant to functions being carried out under the POCA or any other enactment relating to criminal conduct or benefit from criminal conduct;	POCA	97(2)(a)
The disclosure is to an attorney-at-law for the purpose of obtaining legal advice or for the purpose of the attorney-at-law giving legal advice and only where disclosures in this regard are not made with the intention of furthering a criminal purpose;	POCA TPA	97(2)(c); 97(3)(a) 17(2)(a); 17(4)(a)
The disclosure is made pursuant to functions being carried out under the POCA or any other enactment relating to criminal conduct or benefit from criminal conduct;	POCA	97(2)(b)
The disclosure is to the Competent	POCA	97(2)(e)

[238] POCA section 97(2); TPA section 17(2)

Authority;		
The disclosure is to any person in connection with legal proceedings or contemplated legal proceedings;	POCA	97(3)

272. Apart from the foregoing exceptions, a financial institution is under strict obligations not to disclose to any person, the fact that it has made a required disclosure pursuant to sections 94 and 100 of the POCA, or made a disclosure pursuant to section 16(2) or 16(3) of the TPA and must comply with all directions given to it by the relevant authorities[239]. Based on the wording of the tipping off provisions in the POCA and TPA, the obligations thereunder are also applicable to the officers and employees of financial institutions.

Protected disclosures

273. The POCA has two provisions treating with the issue of protected disclosures. The first of these provisions can be found at section 100(3). This section states that disclosures made in the circumstances outlined in **section 100** are protected from being interpreted as breaches of any disclosure restraints however imposed. The second provision is **section 137** which contains a more broadly worded all embracing statement that no civil or criminal proceedings for breach of confidentiality may be brought, nor any professional sanction for such breach taken, against any person, or a director or employee of an institution, who provides or transmits information requested by or submits reports to, the enforcing authority under POCA. A similar provision to section 137 can be found at section 16(7) of the TPA.

274. A financial institution should decline to do any business (including opening an account) with a potential customer or take the measures outlined above at paragraph 113 in relation to existing customers if there are serious doubts about the bona fides of the individual or criminal

[239] POC (MLP) Regulations, regulation 3(6); TP (Reporting Entities) Regulations, regulation 19

involvement is suspected[240]. Where criminal involvement is suspected, the financial institution should also seek to retain copies of relevant identification or other documents, which may have been presented, and should consider reporting the offer of suspicious funds to the Designated Authority[241] . Where a business relationship has already commenced and the customer fails to provide requested follow-up information, the relationship should be legally terminated unless otherwise advised by the law enforcement authorities. (See paragraph 114) In seeking to terminate the relationship, financial institutions should be mindful of the prohibition against "tipping off" or unauthorised disclosures outlined under the POCA[242] and the TPA[243] and should therefore be careful not to "tip off" customers, potential customers or any unauthorized person, where a suspicion has been formed by the financial institution that an offence is being attempted or has been or is being committed. Under POCA a "tipping off" offence occurs where a disclosure likely to prejudice investigations, either in relation to a required disclosure or a money laundering investigation, has taken place. Under the TPA a similar offence occurs where 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 in relation to a report made under the TPA, is disclosed.

Where an institution forms the suspicion that criminal activity is taking place after a business relationship is established with a customer, the institution should seek to legally terminate arrangements where it is of the view that continuing the relationship could lead to legal or reputational risks due to the suspected criminal activity. (See paragraph 110) See also paragraph 217(d) for guidance on transactions that though not suspicious, raise questions or are flagged for closer scrutiny and which in that case are still conducted.)

SECTION X – CONCLUSION

[240] POC (MLP) Regulations, 2007 & amended 2013, regulation 7(1)(b); See also TP (Reporting Entities) Regulations, 2010 regulation 5 (a); See also FATF Recommendation 10.
[241] POC (MLP) Regulations, regulation 7(1)(b); See also FATF Recommendation 10.
[242] POCA sections 97 and 104
[243] TPA section 17 (2) &(3)

275. These Guidance Notes are intended to bring to the attention of financial institutions, the **minimum standards** required of an effective programme to detect and deter money laundering and terrorist financing. The Bank of Jamaica wishes to emphasize that the AML and CFT policies and procedures of financial institutions should be developed in accordance with the law and these Guidance Notes inclusive of Appendices, giving consideration to each institution's risk profile, internal procedures and policies, and where applicable the policies of the financial group in which the financial institution resides.

SECTION XI - APPENDICES

APPENDIX I - Criteria for Designation as a 'Permitted Person' Under Section 101A of the POCA

1. According to the Guidance from the Ministry of National Security[244], the criteria stipulated below must be fulfilled in order for the applicant to qualify for 'permitted person' status under section 101A of the Act.

(a) Demonstration of a true need for 'permitted person' status. Information provided in support of this requirement must include data on the frequency of cash transactions in excess of the prescribed amount carried out by the applicant over the past 3 years preceding the application;

(b) In the case of financial institutions, the applicant must have a Regulator, which monitors the entities day to day operations on an active basis. It must be licensed

[244] Developed by the Ministry of National Security in August, 2014

and the substantial owners, directors and managers (as applicable) should be subject to statutory 'fit and proper' requirements and processes;

(c) In the case of financial institutions, such applicants should produce written confirmations from the respective Regulator and the Financial Investigation Divisions (FID) that there is no objection to the granting of 'permitted person' status to the applicant;

(d) In all cases, the applicant must have proper and demonstrable systems and mechanisms in place against money laundering and counter-terrorism financing (ML/CTF), that protect the applicant from the risks of the applicant being involved in money laundering or the combating of the financing of terrorism. The Ministry has indicated further that at a minimum, this should include documented measures to ascertain the identity of persons carrying out transactions of this nature; recording of transactions in detail; staff training; appointed officer to monitor compliance with the procedures, as well as procedures for reporting suspicious transactions to the Designated Authority under POCA; and obtaining authorized consent where necessary;

2. The Ministry has further indicated that -

(a) all applications for 'permitted person' status are considered on the individual merit of each case.

(b) the Minister may withdraw or rescind any Order granted under section 101A in any case where:

(i) The applicant has provided misleading information in making an application;

(ii) Either the FID or the Regulator advises the Minister that the exemption should no longer apply to the Applicant;

(iii) The applicant has failed to implement or adhere to the procedures referred to at 4 above, and

(iv) The applicant or any of its principals, shareholders or managers has been charged or convicted of any crime relating to the operations of the Applicant.

Full details of the criteria to be met to obtain 'permitted person' status and the requisite application procedure and other details can be accessed from the Ministry of National Security.

APPENDIX II – Advisory issued by BOJ in May 2014

Advisory

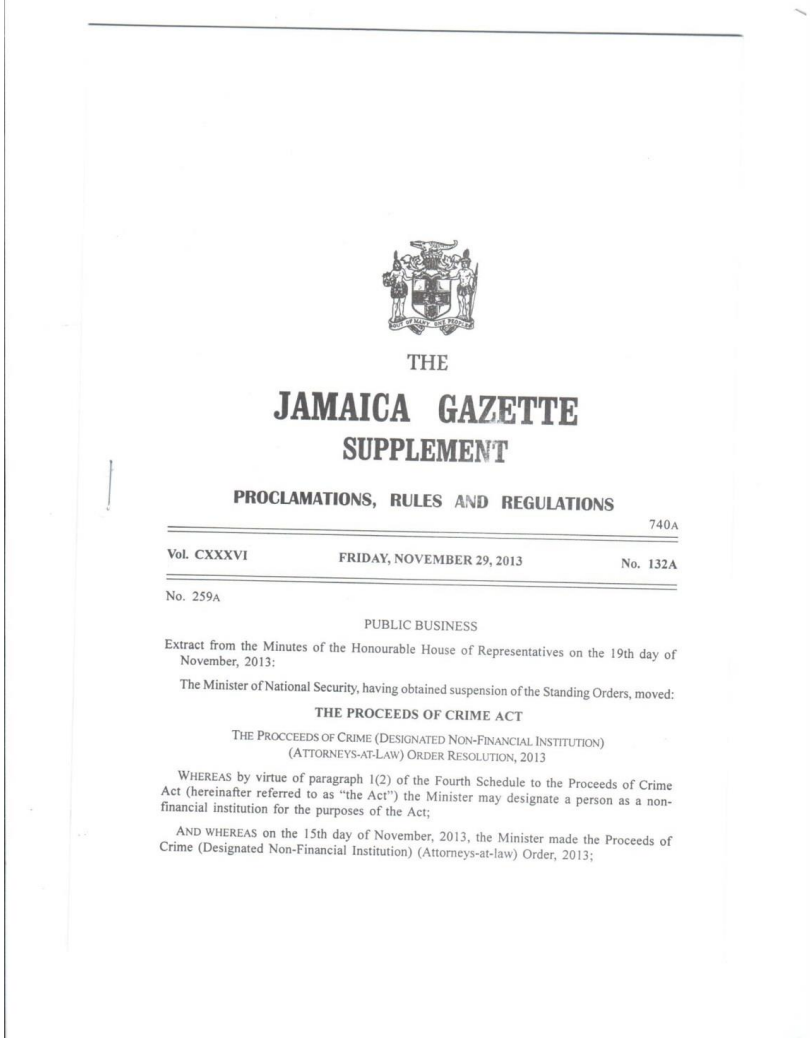
Section 101A Proceeds of Crime Act

Based on information that has come to the Bank's attention, the Bank wishes to provide the following advisory on carrying out banking cash transactions in excess of J$1,000,000.00.

Section 101A of the Proceeds of Crime Act states that, a person shall not carry out a cash transaction in excess of J$1,000,000.00, unless such transaction is undertaken with a permitted person. A 'permitted person' includes a bank licensed under the Banking Act, a licensed deposit taking institution regulated by Bank of Jamaica, a person licensed under the Bank of Jamaica Act to operate an exchange bureau or any other person that may be designated by the Minister as a 'permitted person' by Ministerial Order.

The Bank wishes to clarify that 'permitted persons' may carry out cash transactions in excess of the cash transaction limit threshold. While therefore a permitted person will need to ensure that in transacting business with the public or its customers, it does not facilitate a breach of the law, banks and other licensed deposit taking institutions should not refuse to carry out cash transactions solely on the basis of a cash transaction exceeding the threshold limit.

APPENDIX III – Designation Orders (Paragraph 81)



THE

JAMAICA GAZETTE

SUPPLEMENT

PROCLAMATIONS, RULES AND REGULATIONS

740A

Vol. CXXXVI FRIDAY, NOVEMBER 29, 2013 No. 132A

No. 259A

PUBLIC BUSINESS

Extract from the Minutes of the Honourable House of Representatives on the 19th day of November, 2013:

The Minister of National Security, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (ATTORNEYS-AT-LAW) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as "the Act") the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution of this Honourable House:

NOW THEREFORE, BE IT RESOLVED by this Honourable House as follows:

(i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order Resolution, 2013.

(ii) The Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order, 2013, which was laid on the Table of the House on the 19th day of November, 2013, is hereby affirmed.

(Mr. Jolyan Silvera, MP, St. Mary, Western, entered and took his seat).

(Mr. William J. C. Hutchinson, CD, MP, St. Elizabeth, North Western, entered and took his seat).

Seconded by: Mr. Mikael Phillips.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259B

PUBLIC BUSINESS

Extract from the Minutes of the Honourable Senate on the 29th day of November, 2013:

The Minister of Justice, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (ATTORNEYS-AT-LAW) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as "the Act") the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution:

NOW THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:

(i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order Resolution, 2013.

(ii) The Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order, 2013, which was laid on the Table of the Senate on the 28th day of November, 2013, is hereby affirmed.

Seconded by: Senator Alexander Williams.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259C

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (ATTORNEYS-AT-LAW) ORDER, 2013

In exercise of the powers conferred upon the Minister by paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act, the following Order is hereby made:—

1. This Order may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Attorneys-at-law) Order, 2013.

2. With effect from the 1st day of June, 2014, any person to whom paragraph 3 applies is hereby designated as a non-financial institution for the purposes of the Act.

3. This paragraph applies to any person whose name is entered on the Roll of attorneys-at-law pursuant to section 4 of the Legal Profession Act, and who carries out any of the following activities on behalf of any client—

(a) purchasing or selling real estate;

(b) managing money, securities or other assets;

(c) managing bank accounts or savings accounts of any kind, or securities accounts;

(d) organizing contributions for the creation, operation or management of companies;

(e) creating, operating or managing a legal person or legal arrangement (such as a trust or settlement); or

(f) purchasing or selling a business entity.

4. For the purposes of paragraph 3, "securities" has the meaning assigned to it under the Securities Act.

Dated this 15th day of November, 2013.

PETER BUNTING
Minister of National Security.

No. 259D

PUBLIC BUSINESS

Extract from the Minutes of the Honourable House of Representatives on the 19th day of November, 2013:

The Minister of National Security, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (REAL ESTATE DEALERS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as "the Act") the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution of this Honourable House:

NOW THEREFORE, BE IT RESOLVED by this Honourable House as follows:

(i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order Resolution, 2013.

(ii) The Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order, 2013, which was laid on the Table of the House on the 19th day of November, 2013, is hereby affirmed.

Seconded by: Dr. Dayton Campbell.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259E

PUBLIC BUSINESS

Extract from the Minutes of the Honourable Senate on the 29th day of November, 2013:

The Minister of Justice, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (REAL ESTATE DEALERS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as "the Act") the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution:

NOW THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:

(i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order Resolution, 2013.

(ii) The Proceeds of Crime (Designated Non-Financial Institution) (Real Estate Dealers) Order, 2013, which was laid on the Table of the Senate on the 28th day of November, 2013, is hereby affirmed.

Seconded by: Senator Alexander Williams.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259F

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (REAL ESTATE DEALERS) ORDER, 2013

In exercise of the powers conferred upon the Minister by paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act, the following Order is hereby made:—

1. This Order may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Real Eastate Dealers) Order, 2013.

2. With effect from the 1st day of April, 2014, any person to whom paragraph 3 applies is hereby designated as a non-financial institution for the purposes of the Act.

3. This paragraph applies to any person who is issued a licence under the Real Estate (Dealers and Developers) Act authorizing that person to engage in the practice of real estate business in the capacity of a real estate dealer.

Dated this 15th day of November, 2013.

PETER BUNTING
Minister of National Security.

No. 259G

PUBLIC BUSINESS

Extract from the Minutes of the Honourable House of Representatives on the 19th day of November, 2013:

The Minister of National Security, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (GAMING MACHINE OPERATORS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as "the Act") the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution of this Honourable House:

NOW THEREFORE, BE IT RESOLVED by this Honourable House as follows:

(i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order Resolution, 2013.

(ii) The Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order, 2013, which was laid on the Table of the House on the 19th day of November, 2013, is hereby affirmed.

(Miss Olivia Grange, MP, St. Catherine, Central, entered and took her seat).

(Mr. Andrew Holness, MP, St. Andrew, West Central and Leader of the Opposition, entered and took his seat).

Seconded by: Mr. Richard Parchment.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259H

PUBLIC BUSINESS

Extract from the Minutes of the Honourable Senate on the 29th day of November, 2013:

The Minister of Justice, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (GAMING MACHINE OPERATORS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as "the Act") the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution:

NOW THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:

(i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order Resolution, 2013.

(ii) The Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order, 2013, which was laid on the Table of the Senate on the 28th day of November, 2013, is hereby affirmed.

Seconded by: Senator Alexander Williams.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259I

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (GAMING MACHINE OPERATORS) ORDER, 2013

In exercise of the powers conferred upon the Minister by paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act, the following Order is hereby made:—

1. This Order may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order, 2013.

2. With effect from the 1st day of April, 2014, any person to whom paragraph 3 applies is hereby designated as a non-financial institution for the purposes of the Act.

3. This paragraph applies to any person who operates twenty or more gaming machines pursuant to a licence under the Betting, Gaming and Lotteries Act.

4. For the purposes of paragraph 3, "gaming machine" and "prescribed premises" have the meaning assigned to them, respectively, by section 43 of the Betting, Gaming and Lotteries Act.

Dated this 15th day of November, 2013.

PETER BUNTING
Minister of National Security.

No. 259J

PUBLIC BUSINESS

Extract from the Minutes of the Honourable House of Representatives on the 19th day of November, 2013:

The Minister of National Security, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (CASINO OPERATORS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as "the Act") the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution of this Honourable House:

NOW THEREFORE, BE IT RESOLVED by this Honourable House as follows:

(i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order Resolution, 2013.

(ii) The Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013, which was laid on the Table of the House on the 19th day of November, 2013, is hereby affirmed.

Seconded by: Dr. Winston Green.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259K

PUBLIC BUSINESS

Extract from the Minutes of the Honourable Senate on the 29th day of November, 2013:

The Minister of Justice, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (CASINO OPERATORS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as "the Act") the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution:

NOW THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:

(i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order Resolution, 2013.

(ii) The Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013, which was laid on the Table of the Senate on the 28th day of November, 2013, is hereby affirmed.

Seconded by: Senator Alexander Williams.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259L

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (CASINO OPERATORS) ORDER, 2013

In exercise of the powers conferred upon the Minister by paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act, the following Order is hereby made:—

1. This Order may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013.

2. With effect from the 1st day of April, 2014, any person to whom paragraph 3 applies is hereby designated as a non-financial institution for the purposes of the Act.

3. This paragraph applies to any person who operates a casino pursuant to a licence issued under the Casino Gaming Act.

4. For the purposes of paragraph 3, "casino" has the meaning assigned to it under the Casino Gaming Act.

Dated this 15th day of November, 2013.

PETER BUNTING
Minister of National Security.

No. 259M

PUBLIC BUSINESS

Extract from the Minutes of the Honourable House of Representatives on the 19th day of November, 2013:

The Minister of National Security, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (PUBLIC ACCOUNTANTS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as "the Act") the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution of this Honourable House:

NOW THEREFORE, BE IT RESOLVED by this Honourable House as follows:

(i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order Resolution, 2013.

(ii) The Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order, 2013, which was laid on the Table of the House on the 19th day of November, 2013, is hereby affirmed.

(The Minister of State in the Office of the Prime Minister, the Honourable Luther Buchanan, entered and took his seat).

(Dr. Winston Green, MP, St. Mary, South Eastern, entered and took his seat).

Seconded by: Mr. Joylyan Silvera.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 259N

PUBLIC BUSINESS

Extract from the Minutes of the Honourable Senate on the 29th day of November, 2013:

The Minister of Justice, having obtained suspension of the Standing Orders, moved:

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (PUBLIC ACCOUNTANTS) ORDER RESOLUTION, 2013

WHEREAS by virtue of paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act (hereinafter referred to as "the Act") the Minister may designate a person as a non-financial institution for the purposes of the Act;

AND WHEREAS on the 15th day of November, 2013, the Minister made the Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order, 2013;

AND WHEREAS it is provided by paragraph 1(2) of the Fourth Schedule to the Act that every order made under that paragraph shall be subject to affirmative resolution:

NOW THEREFORE, BE IT RESOLVED by this Honourable Senate as follows:

(i) This Resolution may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order Resolution, 2013.

(ii) The Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order, 2013, which was laid on the Table of the Senate on the 28th day of November, 2013, is hereby affirmed.

Seconded by: Senator Alexander Williams.

Agreed to.

I certify that the above is a true Extract from the Minutes.

HEATHER E. COOKE, JP, (MRS.)
Clerk to the Houses.

No. 2590

THE PROCEEDS OF CRIME ACT

THE PROCCEEDS OF CRIME (DESIGNATED NON-FINANCIAL INSTITUTION) (PUBLIC ACCOUNTANTS) ORDER, 2013

In exercise of the powers conferred upon the Minister by paragraph 1(2) of the Fourth Schedule to the Proceeds of Crime Act, the following Order is hereby made:—

1. This Order may be cited as the Proceeds of Crime (Designated Non-Financial Institution) (Public Accountants) Order, 2013.

2. With effect from the 1st day of April, 2014, any person to whom paragraph 3 applies is hereby designated as a non-financial institution for the purposes of the Act.

3. This paragraph applies to any person registered as a public accountant under the Public Accountancy Act, and who carries out any of the following activities on behalf of any client—

(a) purchasing or selling real estate;

(b) managing money, securities or other assets;

(c) managing bank accounts or savings accounts of any kind, or securities accounts;

(d) organizing contributions for the creation, operation or management of companies;

(e) creating, operating or managing a legal person or legal arrangement (such as a trust or settlement); or

(f) purchasing or selling a business entity.

4. For the purposes of paragraph 3, "securities" has the meaning assigned to it under the Securities Act.

Dated this 15th day of November, 2013.

PETER BUNTING
Minister of National Security.

PRINTED BY JAMAICA PRINTING SERVICES (1992) LTD., (GOVERNMENT PRINTERS), DUKE STREET, KINGSTON, JAMAICA

APPENDIX IV - Basic Duties and Responsibilities of the Nominated Officer

The "Nominated Officer" should be responsible for the day-to-day monitoring of the financial institution's compliance with AML/CFT laws, regulations and industry best practices. That officer should possess the requisite skills, qualification and expertise to effectively perform the assigned tasks; and most importantly, he/she should have access to all operational areas and have the requisite seniority and authority to report independently to the board. This duty must be independent of the internal audit function.

The duties and functions of the Nominated Officer should at a minimum include, inter alia, the following:

1. Act as liaison between the financial institution and the Bank of Jamaica and law enforcement agencies (FID, DPP, etc) with respect to compliance matters and investigations;

2. Ensure risk assessments are done by the financial institution; and oversee the risk assessments done by the financial institution to ensure the appropriate risk profiles are established and the relevant measures and mechanisms commensurate with the risks assessed, are implemented; and ensure these assessments are kept up to date and relevant;

3. Evaluate new products and services to determine the level of risk(s) posed by such products and services to the financial institution;

4. Evaluate reports of suspicious/unusual transactions by personnel and ensuring the timely filing of Suspicious Transaction Reports/Suspicious Activity Reports;

5. Coordinate with the financial institution's audit, legal and security departments on AML/CFT matters and investigations; and on matters pertaining to targeted financial sanctions notified by the United Nations Security Council;

6. Prepare report to the Senior Management, and the Board of Directors at least on an annual basis on the effectiveness of the AML/CFT framework. Where applicable this report should also speak to compliance levels with directives pertaining to targeted financial sanctions

notified by the United Nations Security Council (This report should be subject to review by the Bank of Jamaica);

7. Advise business units of proposed or pending regulatory changes;

8. Prepare and update policies and procedures and disseminate information to the financial institution's Board, Management, staff, and other relevant personnel and parties who may be directly or indirectly involved in the operations (and where applicable) the delivery of banking services of the financial institution[245];

9. Oversee and ensure the implementation of compliance programmes;

10. Oversee administrative matters related to Code of Conduct and Compliance with Anti-money Laundering and Terrorist Financing Activities; and

11. Develop training material and coordinate anti-money laundering training/counter terrorist financing training and training in relation to responding to directives to apply targeted financial sanctions notified by the United Nations Security Council.

[245] This grouping includes Consultants; Contractors (pursuant to outsourcing arrangements); Agents (pursuant to agent banking arrangements)

APPENDIX V - Examples of Unusual/Suspicious Activities

1. Provision of Insufficient or Suspicious Information.

2. 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.

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;

3. 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

4. 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;

5. 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.

6. 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.

7. 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.

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

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

9. 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.

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

11. 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.)