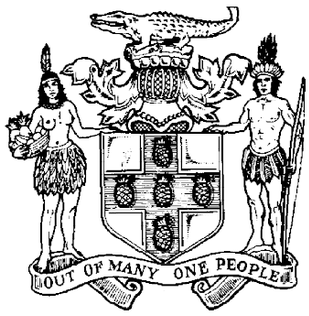

THE

JAMAICA GAZETTE

EXTRAORDINARY

343

Vol. CXLVI **WEDNESDAY, MARCH 29, 2023** **No. 114**

The following Notifications are, by command of His Excellency the Governor-General, published for general information.

PATRICIA RODNEY EVERING, OD (MS.)
Governor-General's Secretary and
Clerk to the Privy Council (Assigned).

GOVERNMENT NOTICES

MISCELLLANEOUS

No. 111

Pursuant to the provisions of the Terrorism Prevention Act, the United Nations Security Council Resolutions Implementation Act and their attendant Regulations, the Minister of Foreign Affairs and Foreign Trade has approved these Guidelines issued by the Financial Services Commission to its regulated businesses.

Signed on the 10th day of January, 2023.

KAMINA JOHNSON SMITH
Minister of Foreign Affairs and Foreign Trade.

No. 112

Pursuant to the provisions of the Proceeds of Crime Act and its attendant Regulations, the Minister of National Security has approved these Guidelines issued by the Financial Services Commission to its regulated businesses.

Signed on the 16th day of February, 2023.

DR. THE HONOURABLE HORACE CHANG
Minister of National Security.

TABLE OF CONTENTS

IER–GUID–2022/09–0002

Foreword

The Financial Services Commission (FSC) has the responsibility for ensuring that regulated businesses in respect of which it exercises the role of Competent Authority are compliant with respect to their Anti-Money Laundering, Counter Financing of Terrorism and Counter Proliferation Financing (AML/CFT/CPF) requirements under the Proceeds of Crime Act (POCA), Terrorism Prevention Act (TPA), United Nations Security Council Resolutions Implementation Act (UNSCRIA) and the regulations attendant to each piece of legislation and as such, periodically updates its Guidelines in accordance with that responsibility.

These Guidelines have been updated to incorporate the 2019 amendments to the AML/CFT/CPF legislation including the United Nations Security Council Resolutions Implementation (Reporting Entities) Regulations, 2019 (UNSCRI-RER), and the updated Financial Action Task Force (FATF) Forty (40) Recommendations and Guidance (2021). Accordingly, these Guidelines inform the FSC's regulated businesses of the measures that must be implemented within their AML/CFT/CPF framework. These measures include:

(a) application of simplified due diligence (SDD) procedures for business relationships or one-off transactions that have been established as low-risk;

(b) amendments to customer due diligence (CDD) obligations;

(c) enhanced countermeasures for customers that are domiciled/resident/incorporated in specified territories;

(d) imposition of additional recordkeeping procedures; and

(e) the requirement to submit reports on proscribed persons under the UNSCRI-RER to the Designated Authority.

The amended legislation requires regulated businesses to immediately freeze the funds, assets and other economic resources that are under their control that are owned, wholly or jointly, or controlled, directly or indirectly, by listed/proscribed persons.

In addition, Competent Authorities are now empowered under POCA in conjunction with the Proceeds of Crime (Money Laundering Prevention) Regulations (POC-MLPR) to impose fixed penalties for specified breaches of the legislation (in *lieu* of criminal sanctions).

This document replaces the FSC's *Guidelines on the Prevention of Money Laundering and Countering the Financing of Terrorism and Proliferation* issued on October 31, 2019. Regulated businesses should, nonetheless, refer directly to the applicable legislation when ascertaining their statutory obligations. These Guidelines are not exhaustive and neither restricts nor limits a regulated business' ability to meet its obligations.

SECTION I—PRELIMINARY PROVISIONS APPLICABILITY AND LEGAL STATUS OF THESE GUIDELINES

Interpretation

In these Guidelines—

"Applicable Legislation" includes—

The Proceeds of Crime Act (POCA);

The Proceeds of Crime (Money Laundering Prevention) Regulations, (POC-MLPR);

The Terrorism Prevention Act (TPA);

The Terrorism Prevention (Reporting Entities) Regulations, (TP-RER);

The United Nations Security Council Resolution Implementation Act, (UNSCRIA);

The United Nations Security Council Resolution Implementation (Reporting Entities) Regulations (UNSCRI-RER);

The United Nations Security Council Resolution Implementation (Asset Freeze—

Democratic People's Republic of Korea) Regulations (DPRK Regulations);

The Financial Services Commission Act (FSCA) and Regulations;

The Insurance Act and Regulations;

The Securities Act and Regulations;

The Trust and Corporate Services Providers Act (TCSPA) and Regulations;

The Financial Investigations Division Act (FIDA);

The Bank of Jamaica Act (BOJA);

The Banking Services Act (BSA);

The Trusts Act;

The Companies Act; and

any other applicable enactment and amendments governing AML/CFT/CPF.

"beneficial owner" means the natural person(s) who ultimately owns or controls a customer and/or the natural person(s) on whose behalf a transaction is being conducted. This includes the natural person(s) who exercise(s) ultimate effective control over a legal person or arrangement.

"Competent Authority" means the person authorized by the Minister to monitor compliance of businesses in the regulated sector and to issue guidelines to these businesses to prevent money laundering, terrorism financing and proliferation financing (ML/TF/PF).

"control" in relation to—

(a) a company, means the power of a person (whether acting alone or jointly with another) to secure, by the holding of, or beneficial entitlement to twenty-five percent or more of the voting rights in the company, so that the affairs of the company are conducted in accordance with the wishes of that person;

(b) any other entity, means the power of a person to determine the policy of the entity or to make a final attachment as to the decisions to be made by that entity.

"*Designated Authority"* means the Chief Technical Director of the Financial Investigations Division (FID) for the purposes of the POCA, TPA and the UNSCRIA.

"designated non-financial business and profession (DNFBP)" means a designated non-financial institution (DNFI).

"designated non-financial institution" means a person who is not primarily engaged in carrying on financial business and who is so designated by the Minister. Such businesses/professions that have been designated are:

(a) Gaming lounges;

(b) Casinos;

(c) Attorneys;

(d) Accountants;

(e) Trust and Corporate Service Providers (TCSPs);

(f) Real Estate Dealers.

"established customer" means a customer with a business relationship for at least twelve (12) months immediately preceding the transaction.

"financial institution" means—

(a) a person engaging in life insurance business or who performs services as an insurance intermediary, in respect of life insurance, within the meaning of the Insurance Act, but does not include an insurance consultant or an adjuster;

(b) a person who is licensed under the Securities Act as a dealer or investment adviser;

(c) a commercial bank as defined in the Banking Services Act;

(d) a merchant bank as defined in the Banking Services Act;

(e) a building society as defined in the Banking Services Act;

(f) a cooperative society which carries on credit union business;

(g) a person licensed under the Bank of Jamaica Act to operate an exchange bureau;

(h) a money transfer and remittance agent or agency (as defined in section 2 of the Bank of Jamaica Act);

(i) a microcredit institution licensed under the Microcredit Act; or

(j) any person declared by the Minister, by order subject to affirmative resolution, to be a financial institution for the purposes of POCA, TPA and UNSCRIA.

"financial services" has the meaning assigned in the FSC Act, 2001.

"listed entity" means any entity for which the Director of Public Prosecutions (DPP) has obtained an Order from a Judge of the Supreme Court and causes to be published in a national newspaper, if the entity—

(a) is included on a list of entities designated as terrorist entities by the United Nations Security Council (UNSC); or

(b) on the basis of the DPP having reasonable grounds to believe that the entity—

(i) has knowingly committed or participated in the commission of a terrorism offence; or

(ii) is knowingly acting on behalf of, at the direction of, or in association with, an entity referred to in the UNSC list of terrorist designated entities.

"money laundering" means an offence under POCA[1], where a person—

(a) engages in a transaction that involves criminal property;

(b) conceals, disguises, disposes of or brings such property into Jamaica;

---

[1]Section 91, POCA (2007)

(c) converts, transfers or removes such property from Jamaica;

(d) acquires, uses or possesses such criminal property; or

(e) attempts, conspires or incites, aids, abets, counsels or procures the commission of any of the acts listed in bullet items (a)—(d) above.

"Nominated Officer" is an employee appointed by a regulated business who performs management functions and has responsibility for the establishment, implementation and maintenance of the systems to detect and prevent ML/TF/PF and the reporting of transactions to the FID.

"orders" means a legal document, approved by a Judge on the request of the DPP, or any other authorized officer, which directs regulated businesses to give specified information and documents to a named constable.

"ordinarily resident in Jamaica" means legally residing in Jamaica for a period of at least six (6) months within a calendar year.

"prescribed amount" means US$15,000.00 or more, or the equivalent in Jamaican or any other currency for an entity regulated by the FSC.

"prescribed holding company" means a holding company licensed by the FSC which holds a subsidiary that is a FSC licensee/registrant[2].

"proliferation financing" means the act of providing funds or financing services which are used in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

"proscribed person or entity" means any such person or entity that is proscribed in accordance with section 3(2)(a) of the UNSCRIA.

"regulated businesses" means businesses falling within the regulatory ambit of the FSC, that is, life insurance, securities, and trust and corporate service providers (TCSPs).

"regulated entities" means a financial institution, financial holding company, or a DNFI which falls under the provisions of POCA, TPA and UNSCRIA.

"relevant authority" means—

(a) the FID or the DPP under the TP (Amendment) Act, 2013; or

(b) has the meaning assigned in section 2 of the UNSCRIA.

"targeted financial sanctions" refers to the required controls and systems with respect to property owned or controlled by listed/proscribed persons/entities. This includes provisions related to asset freezing and prohibitions to prevent funds and other assets from being made available, directly or indirectly, for the benefit of listed/proscribed persons or entities.

"terrorist financing" means the accommodating or facilitating of financial transactions that may be directly or indirectly related to terrorists, terrorist activities and/or terrorist organizations.

"ultimate beneficial owner" means—

(a) in relation to a body corporate, the individual who ultimately owns or controls that body corporate;

(b) in relation to an applicant for business, the individual on whose behalf the applicant for business conducts the business or one-off transaction concerned;

(c) In the case of a trust, settlement or other legal arrangement, the individual who ultimately owns or controls the trust, settlement or other legal arrangement (as the case may be).

"virtual assets" refers to a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. It does not include the digital representation of fiat currencies, securities and other covered financial assets.

"virtual asset service provider" refers to any natural or legal person which as a business conducts any of the following activities for or on behalf of another person:

(a) Exchange between virtual assets and fiat currencies;

(b) Exchange between one or more forms of virtual assets;

(c) Transfer of virtual assets;

(d) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

(e) Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

---

[2]In keeping with pending amendments to the FSC Act.

Any term used in these Guidelines should be construed in accordance with its definition under applicable legislation unless otherwise specifically indicated.

OBJECTIVES

1. These Guidelines have been issued pursuant to section 91(g)(ii) of the POCA, Regulation 20(b) of the TP-RER, and section 14A(b) of the UNSCRIA. The objectives of these Guidelines are to inform regulated businesses that are subject to the supervision of the FSC (in its capacity as Competent Authority) of their responsibilities under the applicable legislation, as well as to identify best practices in AML, CFT and CPF procedures and systems.

2. The Guidelines first came into effect on February 3, 2005 and have been revised on the following dates:

- March 4, 2005
- October 4, 2005
- September 29, 2006
- March 30, 2007
- October 29, 2008
- March 31, 2010
- February 11, 2015
- October 31, 2019

3. This most recent amendment of the Guidelines is effective February 28, 2023.

SCOPE AND APPLICABILITY OF THE GUIDELINES

4. These Guidelines are directed to all financial institutions, prescribed holding companies and DNFIs, as defined by POCA, TPA and UNSCRIA, which are regulated by the FSC.

5. The Guidelines are informed by:

(a) the Applicable Legislation;

(b) the FATF[3] Forty (40) Recommendations, (2021 revision) (and related FATF generated Best Practice Papers); and

(c) other AML/CFT/CPF related international requirements that apply to the regulated entities.

LEGAL STATUS OF THE GUIDELINES

6. On November 12, 2007, the FSC was designated Competent Authority under POCA by the Minister of National Security, specifically with respect to the insurance and securities sectors[4]. The FSC was designated the Competent Authority under POCA on February 28, 2022 for the TCSP sector. Accordingly, the role of the FSC involves overseeing and supervising these regulated businesses in their responsibilities under POCA and POC-MLPR.

7. In May 2015, the FSC was designated Competent Authority for the insurance and securities sectors under the TPA by the Minister responsible for finance and on February 9, 2022 for the TCSP sector.

8. On February 28, 2020, the FSC was designated Competent Authority for the life insurance and securities sectors under the UNSCRIA by the Minister responsible for Foreign Affairs and Foreign Trade.

9. On February 11, 2022, the FSC was designated as Competent Authority for TCSPs under the UNSCRIA by the Minister responsible for Foreign Affairs and Foreign Trade.

10. Under section 91(l)(g) of POCA, Regulation 20(b) of the TP-RER and section 14A(b) of the UNSCRIA, the Competent Authority is required to:

(a) issue guidelines to businesses in the regulated sectors regarding effective measures to prevent money laundering, terrorism financing and proliferation financing respectively; and

(b) monitor the compliance of its regulated businesses.

11. Under Section 91A of POCA, section 18A(2) of the TPA, regulation 9(1) of the UNSCRI-RER a Competent Authority—

(a) shall establish such measures as it thinks fit, including carrying out or directing a third party to carry out, such inspections or such verification procedures as may be necessary;

(b) may issue directions to any of the businesses concerned;

(c) may examine and take copies of information or documents in the possession or control of any of the businesses concerned, and relating to the operations of that business;

(d) may share information, pertaining to any examination conducted by it under this section, with another competent authority, a supervisory authority or the Designated Authority, or an authority in another jurisdiction exercising functions analogous to those of the aforementioned authorities excepting information that is protected from such disclosure.

---

[3]The international body that sets standards, develops and promotes policies to combat money laundering, terrorist financing and other related threats to the integrity of the international financial system.
[4]Limited to financial institutions as defined under POCA.

(e) may require the businesses concerned, in accordance with such procedures as it may establish by notice in writing to those businesses:

(i) if a registration requirement does not already exist under any other law, to register with the competent authority such particulars as may be prescribed; and

(ii) to make such reports to the competent authority in respect of such matters as may be specified in the notice.

(f) conduct a risk assessment of each regulated business.

12. Pursuant to POCA[5], POC-MLPR[6], the TP-RER[7], and the UNSCRI-RER[8], a Court will take notice of these Guidelines, when considering whether a person commits an offence under these pieces of legislation.

13. These Guidelines represent best practices and the minimum acceptable standard for compliance with the AML/CFT/CPF legislation. FSC's regulated businesses may adopt internal controls that are of equivalent or higher standard.

14. Failing to adhere to these Guidelines could result in—

(a) an entity, its principals and/or its officers being deemed unfit to conduct business under the relevant sector legislation;

(b) an institution being deemed to be engaging in unsafe and unsound practices; and/or

(c) the Court holding that a regulated business has not complied with the Applicable Legislation.

15. A conviction for an offence under any of the applicable legislation can constitute grounds upon which the registration, licence or other form of permit may be suspended, cancelled or revoked by the Competent Authority.

SECTION IA—BACKGROUND

MONEY LAUNDERING

16. Money laundering refers to all processes, methods, and transactions designed to obscure the characteristics of criminal proceeds so that it appears to have originated from a legitimate source. There are three stages of money laundering: placement, layering, and integration, which may overlap.

17. Regulated entities have become the major targets of money laundering and terrorist financing operations because of the variety of services and investment vehicles offered that may be utilized to conceal the source of funds.

18. The extent and global impact of criminal activities have required countries to make concerted efforts to defend their institutions, financial systems, economies and citizens by criminalizing the proceeds of these crimes. Consequently, 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. Therefore, a regulated business has the dual responsibility of ensuring that it does not commit the offence of ML, and a statutory obligation to ensure that it takes active, effective, and on-going steps such as the implementation of programmes, policies, procedures and controls for the detection and prevention of ML.[9]

TERRORIST FINANCING

19. 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.

20. Regulated entities engaging in business relationships with terrorists and/or terrorist organizations are exposed to significant legal, operational, and reputational risks. Statutory obligations are placed on regulated entities to ensure that they take active, effective, and on-going steps such as the implementation of programmes, policies, procedures and controls for the detection and prevention of terrorist financing.[10] 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.

21. A key issue for regulated entities therefore, is whether it is able to identify any unusual and/or suspicious transaction that merits additional scrutiny and to record and report such transactions accordingly. In this regard, regulated entities should pay particular attention to the:—

(a) nature of the transaction itself;

(b) parties involved in the transaction; and

(c) pattern of transactions or activities over time.

PROLIFERATION FINANCING

22. Proliferation financing refers to the act of providing funds or financing services which are used in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials.

23. FATF Recommendation 7 requires countries to implement proliferation financing-related Targeted Financial Sanctions (TFS) made under United Nations Security Council Resolutions (UNSCRs). FATF Recommendation 2 requires countries to put in place effective national cooperation and coordination mechanisms to combat the financing of proliferation of weapons of mass destruction (WMD).

---

[5]Section 94(7)(a)
[6]Regulation 2(3), (4) and (5)
[7]Regulation 3(1) and (2)
[8]Regulation 3(1) and (2); Regulation 9(1)(b)
[9]See Regulation 5, POC-MLPR.
[10]Section 18, TPA.

24. The United Nations Security Council (UNSC) has a two-tiered approach to countering proliferation financing through resolutions made under Chapter VII of the Charter of the United Nations (the Charter), which thereby imposes mandatory obligations on United Nations (UN) member states:

(a) global approach under UNSCR 1540 (2004) and its successor resolutions broad-based provisions both prohibiting the financing of proliferation-related activities by non-state persons and requiring countries to establish, develop, review and maintain appropriate controls on providing funds and services related to the export and trans-shipment of items that would contribute to WMD proliferation.

(b) country-specific approach under UNSCR 1718 (2006) and UNSCR 2231 (2015) and their successor resolutions—resolutions against the Democratic People's Republic of Korea (DPKR)[11] and the Islamic Republic of Iran.

25. TFS relating to proliferation financing are applicable to persons designated by the UNSC with the designation criteria being—

(a) persons engaging in or providing support for, including through illicit means, proliferation-sensitive activities and programmes;

(b) acting on behalf of or at the direction of designated persons;

(c) owned or controlled by designated persons; and

(d) persons assisting designated persons or entities in evading sanctions or violating resolution provisions.

26. The FATF Recommendations do not require countries to assess their proliferation financing risks, as the requirement to apply targeted financial sanctions in accordance with FATF Recommendation 7 is not risk-based but rules-based.[12]

SECTION II—AML/CFT/CPF LEGISLATIVE AND REGULATORY FRAMEWORK

Applicable Legislation

The Proceeds of Crime Act (POCA)

27. POCA came into effect on 30th of May 2007 and repealed and replaced the Money Laundering Act, 1998 (MLA) and the Drug Offences (Forfeiture of Proceeds) Act, 1994 (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[13]. Criminal property is any property that constitutes a benefit derived wholly or partially from criminal conduct. Criminal conduct[14] means any conduct constituting an offence in Jamaica, or if committed outside, conduct that would constitute a crime in Jamaica.

28. POCA comprises seven Parts as follows:

(a) Part I treats with the Assets Recovery Agency provisions. Assets Recovery Agency under section 3(1) means the FID of the Ministry of Finance and Public Service (MoFPS) or any other entity so designated by the Minister by Order. The Director of the Agency under section 3(2) of 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.

(b) Parts II, III and IV treat with orders related to the recovery of criminal proceeds such as Forfeiture Orders, Pecuniary Penalty Orders and Restraint Orders, criminal lifestyle and criminal conduct regime and civil recovery of proceeds of unlawful conduct.

(c) Part V treats with the issue of money laundering, related money laundering offences and required disclosures.

(d) Part VI treats with investigatory tools available such as Disclosure Orders, Search & Seizure Warrants, Customer Information Orders and Account Monitoring Orders.

(e) Part VII treats with matters general in nature such as regulation making powers under POCA, Tainted Gifts, Rules of Court, Protection of Persons exercising functions under POCA, the repeal of the MLA and DOFPA and consequential amendments to other enactments.

Specific Areas of Concern under POCA Part V (Money Laundering) for Regulated Businesses

Offences under Part V (Money Laundering)

29. Pursuant to section 92 (1) it is an offence where a person—

(a) engages in a transaction that involves criminal property[15]; or

(b) conceals, disguises, disposes of, or brings into Jamaica, criminal property[16]; or

(c) converts or transfers or removes criminal property from Jamaica

knowingly 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[17].

---

[11]The United Nations Security Council Resolutions Implementation (Asset-Freeze-Democratic People's Republic of Korea) Regulations, 2013 was passed in November, 2013.
[12]See FATF Guidance on Counter Proliferation Financing, February 2018.
[13]Section 91(1), POCA.
[14]Section 2, POCA.
[15]Section 92(1)(a), POCA.
[16]Section 92(1)(b), POCA.
[17]Section 92(1)(c), POCA.

30. Section 92(2) makes it 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.

31. Section 93(1) 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.

32. Section 94(2) makes it an offence for a person failing to make the requisite disclosure within *15 days after the information or matter comes to a person's attention*[18] 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[19], and this knowledge or belief arose in the course of a business in the regulated sector[20] [Suspicious Transaction Report ('STR') obligation].

33. Section 94(4) requires a business in the regulated sector to make and retain, in relation to each customer, for a period of seven years or over, a record of all:

(a) complex, unusual or large business transactions; and

(b) unusual patterns of transactions, whether completed or not, which appear to be inconsistent with the normal transactions carried out by that customer.

34. Section 94A imposes an obligation on regulated businesses to take enhanced measures in respect of transactions with customers domiciled, resident or incorporated in specified territories.

35. Section 95 makes it an offence where the nominated officer fails to make the requisite disclosure within *15 days after the information or matter comes to his 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 the information or other matter on which this knowledge or belief is based or which gives reasonable grounds for such knowledge or belief as the case may be, came to the nominated officer in consequence of a disclosure made under section 94.

36. Under section 97 of POCA the following actions constitute a "tipping off" offence—

(a) Disclosing information with the knowledge or having reasonable grounds to believe that a disclosure has been made or is to be made under section 100. Disclosures in this regard refer to disclosures by regulated businesses and disclosures to an authorized officer[21].

(b) Disclosing information or any other matter with the knowledge or belief that an authorized body is acting or proposing to act in connection with a money laundering investigation that is being or is about to be conducted[22].

37. Section 99 prohibits a Nominated Officer from giving appropriate consent to the doing of a prohibited act, unless an authorized disclosure (under section 100) is made to the Designated Authority and any of the following occurs:

(a) the Designated Authority gives consent to the doing of the act within seven business days;

(b) there is no response from the Designated Authority and seven business days have passed;

(c) consent has been denied but ten days have passed since the denial of consent notice was received.

38. Section 101 makes failing to make a report where cash (which includes bearer-negotiable instruments) exceeding US$10,000 or the equivalent amount in any other currency, is being taken into or out of Jamaica[23], an offence.

Cash Transaction Limits (Section 101A POCA)

39. Section 101A, POCA has introduced a limit of J$1 million (or its equivalent in any other currency) on certain cash transactions unless such transaction is undertaken with a permitted or exempted person or the transaction itself is exempted. The meanings of 'permitted person', 'exempted person' and 'exempted transaction' are indicated below:

(a) A permitted person includes a commercial bank, a merchant bank, a building society, a cambio and any person so designated by virtue of an order from the Minister with responsibility for national security.

(b) An exempted person or exempted transaction means a person or transaction in relation to which the Minister has made an Order. Where the Minister is satisfied that it is in the public interest, the Minister may, by order subject to affirmative resolution, exempt a person or a particular type of transaction.

40. Section 101A (1) states that:

A person shall not:

(a) pay or receive cash in excess of the prescribed amount in transaction for the purchase of any property or services or for the payment or reduction of any indebtedness, accounts payable or other financial obligation; or

(b) artificially separate a single activity or course of activities into a set of transactions so that each transaction involves a payment and receipt of cash that is less than the prescribed amount but which activity or course of activities in the aggregate involves payment and receipt of cash that exceeds the prescribed amount.

---

[18]Section 94(2)(c), POCA.
[19]Section 94(2)(a), POCA.
[20]Section 94(2)(c), POCA.
[21]Section 100(4)(a), POCA.
[22]Section 97(1)(b), POCA.
[23]Section 101(2), POCA.

41. Securities dealers, insurance companies, insurance intermediaries and TCSPs are not permitted persons[24] and are therefore prohibited from engaging in specified cash transactions (as stated above).

42. The Ministry of National Security has set out the procedures by which persons can apply for permitted person status. The process involves the receipt of no objection letters from both the Competent and Designated Authorities.

Specific Areas of Concern under POCA Part VI (Investigations) for Regulated Businesses

Offences under Part VI—Investigations

43. Disclosing information or any other matter with the knowledge or belief that an investigation related to forfeiture, money laundering or civil recovery, is about to be or is being conducted[25].

44. Failure without reasonable excuse to comply with a disclosure order[26].

45. Failure by a financial institution without reasonable excuse, to comply with a customer information order[27].

46. A financial institution making a statement that it knows is false or misleading in a material particulars[28].

47. A financial institution recklessly making a statement that is false or misleading in a material particulars[29].

48. The responsibility for enforcing the provisions of the POCA is shared amongst the FID (in its capacity as the Asset Recovery Agency ('ARA') and as designated authority through its CTD); the DPP; the Police; Customs; the Competent Authorities, and any other person designated by the Minister. The FSC, as the Competent Authority, is responsible for monitoring compliance with the obligations of the POCA for its regulated businesses.

---

[24]Expecting for any entity which has been granted permitted person status by an Order from the Minister of National Security.
[25]Section 104(2), POCA.
[26]Section 112, POCA.
[27]Section 122(1), POCA.
[28]Section 122(3)(a), POCA.
[29]Section 122(3)(b), POCA.

TABLE 1: Areas of Enforcement under POCA and POC—MLPR

AREAS OF ENFORCEMENT	ACT OR REGULATION	RESPONSIBLE AUTHORITY	ADDITIONAL INFORMATION
Threshold Transaction Reporting (TTR)	Reg. 3	CTD of the FID	
Suspicious Transaction Reports (STR) [Required Disclosure]	Sections 94 & 95	CTD of the FID	
Protected and Authorised Disclosures	Section 100	CTD of the FID	
Fixed Penalty Notice	Section 138 (3) & Reg. 21.	Competent Authority	
Account Monitoring Orders	Section 126	ARA; Constable; Officer designated by the Commissioner; Customs Officer; or any other person designated by the Minister	Any of these persons is referred to as "Authorised Officer".
Issuing Guidelines & implementation of AML measures to monitor compliance with the AML laws.	Sections 91 & 91A	Competent Authority	FSC for Securities Dealers, Life Insurance Companies & Intermediaries and TCSPs; BOJ for licensees under the BSA, credit unions, cambios, microcredit institutions and remittance companies; The Public Accountancy Board for Accountants;

TABLE 1: Areas of Enforcement under POCA and POC—MLPR, *contd.*

			General Legal Council for Attorneys; The Real Estate Board for Real Estate Dealers; The Betting, Gaming and Lotteries Commission for the gaming sector; The Casino Gaming Commission for casinos.
Forfeiture & Pecuniary Penalty Orders	Sections 5 – 31	ARA DPP	
Restraint Orders	Sections 32 & 33	ARA DPP	
Seizure of realizable property that is subject to Restraint Order	Section 36	Authorized Officer	In this section, an Authorized Officer is any of these persons: a Constable, a Customs Officer, an Officer of the ARA, any other person designated by the Minister
Recovery Orders pursuant to the Civil Forfeiture Regime	Sections 57 - 71	ARA DPP	
Recovery of Cash in Summary Proceedings	Sections 72 - 81	Authorized Officer	In these sections, an Authorized Officer is any of these persons: a Constable, a Customs Officer, any other person designated by the Minister
Disclosure Orders	Sections 105 - 109	Appropriate Officer	The ARA, an Authorized Financial Investigator, a Constable, a Customs Officer, any other person designated by the Minister
Ancillary Orders	Section 110		
Search & Seizure Warrants	Section 115		
Customer Information Orders	Sections 119 - 121		

49. 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.

Criminal Forfeiture Regime

50. The criminal forfeiture process is initiated after conviction when either the ARA or the DPP applies to the Supreme Court for a forfeiture order or a pecuniary penalty order (PPO). At this point, the Court will make a determination as to whether or not the defendant has a criminal lifestyle[30] and has benefitted from his general criminal conduct. Where the Court determines that the defendant has benefitted from criminal conduct, it shall identify the property that represents the defendant's benefit from criminal conduct and make an order for forfeiture or order the defendant to pay to the Crown an amount equal to the value of his benefit[31]. The offences to which the criminal lifestyle regime applies can be found in the second schedule of the POCA.

Civil Forfeiture Regime

51. The POCA allows for the civil recovery[32] of the proceeds of unlawful conduct including cash. The ARA or the DPP (the enforcing authority) is responsible for matters dealing with the civil recovery of proceeds of crime. Civil recovery proceedings are targeted at the property and not the criminal, who may be deceased or outside of the jurisdiction.

Statutory AML Obligations under The POCA and POC-MLPR

52. Statutory AML obligations under the POCA regime can be found in Part V of the POCA and in the POC-MLPR and require the following:

(a) Filing required disclosures (Suspicious Transaction Reports) where this is applicable in the circumstances and manner prescribed (sections 94–95);

(b) Maintaining a log of all unusual, complex, large or unusual patterns of transactions, whether completed or not, for a period of seven years or over (section 94(4));

(c) Filing of Protected and Authorized Disclosures and request for appropriate consent (sections 91, 99 and 100);

(d) Filing TTRs(reg.3(l));

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

(f) Complying with a requirement or direction issued by the Competent Authority (section 91A(2));

(g) Making the required cross border currency report in the manner indicated by the Designated Authority[33] (reporting threshold is over US$10,000 or its equivalent in any other currency.) (section 101);

(h) Conducting customer due diligence (CDD) (reg. 7 and 7A); and

(i) Complying with other AML operational and regulatory controls under the POC-MLPR.

Suspicious Transaction Reports (STRs) (sections 94-95 POCA)

53. 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 designated authority.

54. The circumstances are as follows—

(a) There is knowledge or belief, or there are reasonable grounds for knowing or believing, that another person has engaged in a transaction that could constitute or be related to money laundering (Section 94(2)(a));

(b) 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)); and

(c) The person is required to disclose as soon as is reasonably practicable, and in any event within fifteen (15) days, after the information or other matter comes to him.

55. Under Section 95, there is an obligation for the Nominated Officer to make a required disclosure to the Designated Authority, if:

(a) the Nominated Officer knows or believes, or has reasonable grounds for knowing or believing, that another person has engaged in a transaction that could constitute or be related to money laundering; and

(b) the information or other matter on which his knowledge or belief is based or which gives reasonable grounds for such knowledge or belief, as the case may be, came to the Nominated Officer in consequence of a disclosure made under section 94.

56. With regards to the **STR obligations,** regulated businesses should note:

(a) There is a maximum 30-day period for institutions to file a report with the Designated Authority (that is, 15 days from the date on which the suspicion is formed by the employee who dealt with the transaction 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) Regulated entities have a duty to make a required disclosure in relation to suspicious transactions which arise in the course of the regulated business;

---

[30]Section 6, POCA.
[31]Section 5, POCA.
[32]Part IV, POCA.
[33]Section 101(2), POCA.

(c) Required disclosures are to be made in the manner specified by the Designated Authority *via* the FID's reporting portal-goAML;

(d) In 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;

(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[34];

(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.

Protected and Authorised Disclosures

57. For persons in the non-regulated sector, the provision to make a disclosure in relation to suspicious transactions or activities is contained in section 100 of the POCA. The conditions on which a person can make this report are as follows:

(a) the information or other matter disclosed was obtained in the course of the reporting person's trade, profession, business or employment;

(b) the information or other matter causes the person making the disclosure to know or believe, or to have reasonable grounds for knowing or believing that another person has engaged in money laundering; and

(c) the disclosure is made to an authorized officer[35] or Nominated Officer as soon as is reasonably practicable after the said information or other matter comes to the person making the disclosure.

58. Section 100(4) allows persons in both the regulated and non-regulated sectors to make an authorized disclosure to an authorized officer or nominated officer before carrying out a prohibited act and to seek appropriate consent (sections 91 and 99) to conduct the prohibited act.

59. A person does not commit a money laundering offence (under sections 92 and 93) if the person has made an authorized disclosure and has the appropriate consent to act.

THE POC-MLPR

60. Most of the AML operational and regulatory control requirements are in the Regulations as discussed below.

Threshold Transaction Reporting (TTR)

61. Regulation 3(1) sets out the threshold reporting requirements for financial institutions[36] to report all cash transactions involving the "prescribed amount", as per the limits that have been tiered in relation to financial institutions[37]. Cash transaction reporting requirements are not applicable to cash transactions carried out by:

(a) a Ministry, Department of Government, statutory body or authority;

(b) a company in which the Government or an agency of Government is in a position to influence the policy of the company;

(c) an Embassy, High Commission, consular office or organization to which the Diplomatic Immunities and Privileges Act apply; or

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

62. A financial institution is required to file a TTR within fifteen (15) days of the end of each month on each cash transaction involving the prescribed amount. If there is no such transaction during that month, the institution is required to submit a NIL report to the FID;

63. Regulation 4(2) allows exemptions from the requirement of filing TTRs in relation to established customers. An application must be made to the Minister with responsibility for finance, who is vested with the authority to grant such an exemption. Such exemption would be considered where:

(a) the transaction or series of transactions involve the deposit into, or withdrawal of monies held by an established customer from an account in a financial institution;

(b) the customer carries on:—

(i) a business declared by the Minister by order to be an entertainment business or a hospitality business for the purposes of this Act; or

(ii) a retail business, not including the sale of motor vehicles, vessels, farm machinery or aircraft;

(c) the account through which the transactions are conducted is maintained for the purpose of such business; and

(d) the amount of money involved is not over and above an amount that is reasonably commensurate to the lawful activities of the customer.

---

[34]Section 94(4)(b), POCA.
[35]In this section, an authorized officer is an officer of the FID, a constable or customs officer.
[36]This requirement to file TTRs is limited to financial institutions and has not been extended to DNFIs
[37]The prescribed amount for entities regulated by the FSC is US$15,000 (Regulation 3(8)).

64. The threshold reporting limits[38] for financial institutions are as follows:—

(a) Financial institutions other than cambios and remittance companies—US$15,000 or more or the equivalent amount in any other currency;

(b) Cambios or bureau de exchange—US$8,000 or more or the equivalent amount in any other currency;

(c) Remittance companies—US$5,000 or more or the equivalent amount in any other currency.

65. Under Regulation 3(3) 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.

66. The Designated Authority has the power to issue directions to a regulated business in relation to matters arising from TTRs and STRs filed[39]. These directions can be issued in relation to—

(a) previous or current reports;

(b) the provision of information required in such reports;

(c) the provision of additional information in response to queries concerning specific matters arising from the reports including:

(i) due diligence procedures followed in relation to a specific transaction;

(ii) persons authorized to sign on a specific account;

(iii) errors identified in the report; or

(iv) such other matters specified in the directions.

KYC/CDD requirements

Risk Profile

67. Regulated businesses are required to establish a risk profile for all business relationships and one-off transactions[40]. The basis on which such profiles are established should be guided by the respective risk assessments[41] undertaken by regulated entities. Note that high-risk relationships or transactions as prescribed under Regulation 7A include the following—

(a) An individual carrying out certain state functions including politically exposed persons (PEPs);

(b) Trustees;

(c) A person who is not ordinarily resident in Jamaica;

(d) A company having nominee shareholders, or shares held in bearer form; and

(e) A member of such other class or category of persons as the supervisory authority may specify by notice published in the *Gazette*.

Standard Due Diligence

68. Regulated businesses 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—

(a) business, trade or profession;

(b) risk profile; and

(c) stated source of funds involved in the transaction.

69. Regulation 7A also requires regulated businesses to verify the identity of the transacting party as well as the source of funds for each transaction conducted.

70. Regulation 7(5) defines "customer information" to include the applicant for business's full name, current address[42], taxpayer registration number or other reference number, date and place of birth and mother's maiden name (in the case of a natural person) and, where applicable, the information referred to in regulation 13(l)(c).

71. Regulation 7(l)(b) prescribes that if a regulated business is unable to verify an applicant for business identity within 14 business days after first contact, even if there are no reasonable grounds to believe that the business relationship or one-off transactions constitutes ML, the business relationship should be terminated (unless conducted with the permission of the FSC) and an assessment is to be made as to whether a disclosure is required under section 94/95 of POCA.

72. In any case, where there is a belief that the funds involve criminal property, and there is a belief that the carrying out of required due diligence procedures might alert the applicant of such suspicion, the regulated business should discontinue conducting the CDD and instead file a STR to the FID.

---

[38]Regulation 3(7) and (8), POC-MLPR (2007).
[39]Regulation 3(6), POC-MLPR.
[40]Regulation 7A, POC-MLPR.
[41]Section IV of the Guidelines.
[42]This must be the customer's current permanent address.

Simplified Due Diligence (SDD) Measures

73. Regulation 7A(5A) provides for the application of SDD measures when the regulated business has made a determination that both the applicant for business and the product being accessed by the applicant are low risk. SDD is the application of reduced CDD measures. A regulated business is still expected to identify the applicant for business and to take reasonable measures in verifying the identity of the applicant despite the utilization of SDD procedures.

Additional KYC/CDD Requirements

74. The following KYC/CDD requirements must be applied:

(a) Periodic updates of customer information must be carried out at least once every seven (7) years or at more frequent intervals as warranted by the risk profile of the business relationship. This is applicable to existing and new customers. Updates to customers' information, where accounts were opened prior to March 29, 2007 are restricted to identification information (except for high risk customers)[43]. Identification information includes address verification. Where customer information is not updated as required, then the business relationship shall not proceed any further and an assessment should be made as to whether or not a disclosure is required under sections 94 and 95 of POCA;

(b) Transaction verification procedures must be applied particularly in the circumstances specified in regulation 7(3) which include:

(i) cases where the transaction involves cash at or above the prescribed amount;

(ii) transactions appear to be linked;

(iii) wire transfer transactions are being conducted;

(iv) there is doubt about the accuracy of any previously obtained evidence of identity; or

(v) a required disclosure (STR) is to be made;

(c) Enhanced moneylaundering countermeasures are required for any business relationship or transaction with a person/ entity that is resident, domiciled or incorporated in a specified territory (Regulation 7B);

(d) 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, POC-MLPR);

(e) 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 (Regulations 11, 12 and 13, POC-MLPR);

(f) For insurance contracts, the beneficiary must be identified, and the identity verified. Verification of the identity of the beneficiary can be done at the time of the pay out of the funds. (Regulation 13, POC-MLPR);

(g) Regulated businesses are prohibited from maintaining anonymous, fictitious or numbered accounts (Regulation 16, POC-MLPR);

(h) Regulated businesses must ensure that the CDD update requirements are applied to existing customers;

(i) Regulated businesses 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.

Wire Transfers

75. For wire transfers or any other electronic funds transfers, accurate records must be received and retained throughout the payment process and chain on the following:

(a) Correct Name;

(b) Address;

(c) Account number (where applicable);

(d) Persons involved;

(e) Reference number assigned to the transaction; and

(f) Instructions given in relation to the transfer.

76. There is a requirement to implement risk-based policies and procedures for determining whether to execute, reject or suspend the transfer where the identification and verification procedures have not been satisfied.

77. For transfers exceeding US$500 (or its equivalent), there is a requirement to identify and verify the identity of the recipient. Relevant identity information includes: national identification number, the customer identification number or the date and place of birth of the person who places the order, the account holder and every recipient of the funds transferred (Regulation 9(2A)).

78. It is a requirement that the business from which the transfer originates must provide the KYC details to the business to which the funds are transferred within three business days of being requested so to do by the business to which the funds are transferred (Regulation 9 (2B)).

---

[43]Regulation 7(1)(c) and (d), POC-MLPR; Regulation 19, POC-MLPR.

Record Keeping

79. Regulated businesses must ensure the retention of records of identification and all relevant financial business. In relation to all relevant financial business, a record of each transaction, all correspondence, analysis undertaken, and account files shall be kept in such manner and form that shall facilitate the reconstruction of each transaction. Such records should be retained for a period of seven (7) years commencing on the date on which the relevant financial business was completed, or the business relationship was terminated (whichever was terminated later) or for such other period as may be specified by the Designated Authority. The records should be made available to the Designated Authority or Competent Authority within seven (7) days of a request. (Regulation 14, POC-MLPR).

TERRORISM PREVENTION ACT, 2005 ("TPA")

80. The TPA was passed in 2005, and amended in 2010, 2011, 2013 and 2019. The Act outlines the following as financing offences:—

(a) Directly or indirectly, wilfully and without lawful justification or excuse, collects property, provides or invites a person to provide, or makes available, property or financial 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 or for the benefit of any entity known to be committing or facilitating any terrorist activity;

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

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

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

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

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

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

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

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

(g) Facilitating terrorist activity including:

(i) Leaving or attempting to leave Jamaica in order to facilitate or commit a terrorism offence; or

(ii) Providing any financial or other services to facilitate any person leaving or attempting to leave Jamaica in order to carry out a terrorism offence (section 8).

81. 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.

82. 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[44]—

(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.

(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 obtained 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.

---

[44]Section 2(2) and (7), TPA.

83. The TPA also requires that reporting entities:—

(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; and report to the Designated Authority[45] at least once in every four (4) calendar months or in response to a request made by the Designated Authority, whether or not they are in possession or control of such property[46]. [Listed Entity Report]

A listed entity is one which the court so designates upon an application by the DPP in respect of:

(i) an entity designated as a terrorist entity by the UNSC; or

(ii) an entity which the DPP 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[47];

(b) Report all suspicious transactions to the Designated Authority [Suspicious Transaction Report][48];

(c) Make and retain for a period not less than seven (7) years, a record of all:

(i) Complex, unusual or large business transactions; and

(ii) Unusual patterns of transactions, whether completed or not, which appear to be inconsistent with the normal transactions carried out by that customer[49].

(d) Implement enhanced monitoring in respect of transactions with customers domiciled, resident or incorporated in specified territories[50].

(e) Ensure that high standards of employee integrity are maintained, and that employees are trained on an on-going basis regarding their responsibilities under the Act[51].

(f) Establish and implement programmes, policies, procedures and controls, establish programmes for training of employees on a continuous basis, for enabling them to fulfil their duties under the TPA.

(g) Designate a Nominated Officer at management level who should arrange for independent audits to ensure that compliance programmes are effectively implemented[52].

(h) Apply targeted financial sanctions with respect to any property owned or controlled by or on behalf of a listed entity or derived or generated from such property.[53]

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

TABLE 2—AREAS OF ENFORCEMENT UNDER THE TPA

AREAS OF ENFORCEMENT	ACT OR REGULATION	RESPONSIBLE AUTHORITY
Listed Entity procedures	Sec. 14	DPP
Prohibition to deal with freezable assets	Sec. 14(4A)	FID
Duty of entities to file a Listed Entity Report	Sec. 15	FID

[45]The CTD of the FID is the Designated Authority.
[46]Section 15, TPA
[47]Section 14, TPA
[48]Section 16, TPA
[49]Section 16(2), TPA
[50]Section 16A, TPA
[51]Section 18, TPA
[52]Section 18, TPA
[53]Section 14 (4A), TPA

TABLE 2—AREAS OF ENFORCEMENT UNDER THE TPA, *contd.*

Duty to maintain an unusual transactions log	**Sec.16(2)**	**Competent Authority**
Duty to file STRs	**Sec. 16(3)**	**FID**
Tipping off	**Sec. 17**	**FID**
Implementation of regulatory controls to prevent TF	**Sec.18**	**Competent Authority**
Account Monitoring Orders	**Sec. 19 & 20**	**Relevant Authority[54]**
Examination and Production Orders	**Sec. 21**	**Relevant Authority**
Search Warrant	**Sec. 23-27**	**A Constable named in the Warrant**
Forfeiture Orders	**Secs. 28-33**	**Relevant Authority**
Restraint Orders	**Secs. 34-43**	**Relevant Authority**
Disposal (i.e. resolution of) property seized, restrained etc.	**Sec. 44**	**Relevant Authority**

85. 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 34–43), Search Warrants (sections 23–27), Examination and Production Orders (sections 21 and 22) and Account Monitoring Orders (sections 19 and 20).

TERRORISM PREVENTION (REPORTING ENTITIES) REGULATIONS, 2010

86. The TP-RER were promulgated in March 2010, and later amended in 2011, 2013 and 2019. These Regulations outline the operational procedures that must be maintained by regulated businesses particularly for the commencement of a business relationship or conducting a one-off transaction. These Regulations largely mirror the POC-MLPR and require regulated businesses to:

(a) establish and maintain appropriate procedures in relation to establishing a risk profile for all business relationships and one-off transactions;

(b) identification of customers (including identification of the agent, ultimate beneficial owner or person who ultimately controls a legal person);

(c) record-keeping (minimum 7-year retention period);

(d) internal controls; and

(e) training of employees.

UNITED NATIONS SECURITY COUNCIL RESOLUTIONS IMPLEMENTATION ACT, 2013

87. The United Nations Security Council Resolutions Implementation Act was passed in November 2013 and is intended 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.

88. This Act is an enabling legislation that forms the basis for Jamaica to respond to directives or resolutions issued by the UNSEC by promulgation of the requisite Regulations under this Act.

89. The Act provides for the following:—

(a) a duty on regulated entities to determine whether or not they are in possession of property for a person prescribed under Regulation 3 and to report whether they are, or not, in possession of property for a person who is so prescribed[55]. These reports are to be made to the Designated Authority, which is defined in the Act, to be the CTD of the FID[56] .

[54]The Relevant Authority is either the DPP or the FID.
[55]Section 5, UNSCRIA.
[56]Section 5(1), UNSCRIA.

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[57], (section 5(6)). These reports are due once every four calendar months. Reports are also due upon request of the Designated Authority[58].

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

(c) Restrains persons from dealing directly or indirectly with any assets that are owned or controlled by or on behalf of, or at the direction of, a proscribed person. It also prevents persons from entering into or facilitating, directly or indirectly any transaction in respect of these assets. No person should provide any financial or other related services with respect to these assets or to make any property or any financial or other related service available for the benefit of a proscribed person or convert any such property or take steps to convert or disguise that the property is owned or controlled by or on behalf of the person or entity (section 8A as amended, 2019).

(d) 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.

(e) 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 (section 15) however a person is not required to give any information or document in response to a request, if to do so would violate legal professional privilege[59].

(f) 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 UNSCR (section 3).

90. When a directive or resolution is issued from the UNSC mandating members to take certain actions and/or refrain from activities pursuant to such directive or mandate, Jamaica would then issue the requisite Regulations under this Act within 30 days giving effect to such a decision and outlining the specific parameters of compliance (section 3). To give more immediate effect to the UNSCR, section 3A provides for the DPP to make an application to a Judge of the Supreme Court for an order to declare a person/entity to be a proscribed person/entity. Such an order will remain in effect until the passage of the relevant regulations.

91. The UNSC Resolutions Implementation (Asset Freeze—Democratic People's Republic of Korea) Regulations, 2013[60] were issued pursuant to section 3 of the Act and these Regulations outline Jamaica's mandates in relation to the directives of the UNSC regarding the DPRK 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.

92. 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:

(i) an entity designated in Annex I or Annex II to UNSEC Resolution 2087 (2013); or

(ii) an entity designated by the UN Sanctions Committee or by the UNSC for the purposes of paragraph 5(a) of UN Resolution 2087 (2013) as a person in respect of which countries must freeze funds immediately, or other financial assets and economic resources which are in their territories, owned or 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)).

93. 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).

UNITED NATIONS SECURITY COUNCIL RESOLUTION IMPLEMENTATION (REPORTING ENTITIES) REGULATIONS, 2019

94. The UNSCRI-RER was passed in 2019 and provides mainly for the reporting framework to be instituted by reporting entities.

95. Regulation 5 maintains the identification and verification procedures required under the TP-RER and the POC-MLPR.

96. Regulation 6 provides the Designated Authority with the powers to modify the reporting forms and to allow for electronic submission of reports.

---

[57]Regulation 5(3B), UNSCRI-RER, except to the regulator of the reporting entity.
[58]Section 5(3), UNSCRIA.
[59]Section 14(7), UNSCRIA.
[60]Schedule to the UNSCRIA, 2013.

97. Regulation 8 gives powers to the Designated Authority to give directions to reporting entities with respect to reporting requirements.

98. Regulation 9 sets out the functions of the Competent Authority which include the powers to:

(a) Monitor compliance;

(b) Issue directions; and

(c) Examine and take copies of information or documents in the possession or control of a reporting entity.

TABLE 3—Areas of Enforcement under UNSCRIA, 2013, UNSC Implementation (Asset Freeze-DPRK) Regulations, 2013 and UNSCRI-RER, 2019

AREAS OF ENFORCEMENT	ACT OR REGULATION	RESPONSIBLE AUTHORITY	ADDITIONAL COMMENTS
Duty of entities to report	Sec. 5	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)	FID	
Reporting entities are 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)	FID Competent Authority	
Reporting to the Designated Authority whether or not there is possession or control of assets owned or controlled by or on behalf of a designated entity.	Sec.5(3)	FID	
Complying with a direction of the Designated Authority in making a report under section 5(3).	Sec. 5(4)	FID	
Injunction to prevent breach of an implementing regulation	Sec. 7	Attorney General	
Restricts persons from dealing with assets of proscribed person or entity	Sec. 8A	FID	
Implementation of regulatory controls	Sec. 21 & UNSCRI-RER	Competent Authority	.

TABLE 3—Areas of Enforcement under UNSCRIA, 2013, UNSC Implementation (Asset Freeze-DPRK) Regulations, 2013 and UNSCRI-RER, 2019, *contd.*

to ensure compliance			
Contravention of a UN sanction enforcement law.	Secs. 10 & 11	Relevant Authority	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.
Permission to use or deal with a freezable asset.	DPRK Reg. 7	Ministry with portfolio responsibility for Foreign Affairs and Foreign Trade 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	DPRK Regs. 4, 5 & 6	Office of the Director of Public Prosecutions (ODPP)	

FINANCIAL SERVICES COMMISSION ACT, 2001

99. The FSC was established for the purpose of protecting customers of financial services and therefore has the following responsibilities:

(a) supervise and regulate prescribed financial institutions;

(b) promote the adoption of procedures designed to control and manage risk, for use by the management, boards of directors and trustees of such institutions;

(c) promote stability and public confidence in the operations of such institutions;

(d) promote public understanding of the operation of prescribed financial institutions; and

(e) promote the modernization of financial services with a view to the adoption and maintenance of international standards of competence, efficiency and competitiveness.

100. Additionally, the FSC is mandated to implement measures designed to reduce the possibility of a prescribed financial institution being used for any purpose connected with an offence involving fraud, theft or money laundering.

FINANCIAL INVESTIGATIONS DIVISION ACT, 2010

101. 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 FID is the Designated Authority to receive reports under the POCA (section 91(l)(h); the TPA (section 15)); and the UNSCRIA (section 5(1)). FID statistics and publications including advisories to regulated entities can be accessed from its website at www.fid.gov.im.

102. On June 5, 2014, the FID became a member of the Egmont Group of Financial Intelligence Units.

CRIMINAL JUSTICE (SUPPRESSION OF CRIMINAL ORGANIZATIONS) ACT, 2014

103. 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

104. 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 April 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 medical, therapeutic or scientific purposes.

105. In this regard the following should be noted:—

(a) The Cannabis Licensing Authority (CLA) 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. The CLA is also charged with ensuring that regulations made do not contravene Jamaica's international obligations;

(b) The possession of over 2 ounces of cannabis is 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 and Mining (section 7C).

LAW REFORM (FRAUDULENT TRANSACTIONS) (SPECIAL PROVISIONS) ACT, 2013

106. This Act makes special provisions for offences relating to Advance Fee Fraud (*i.e.* Lottery scamming) and other fraudulent transactions.

CYBER CRIMES ACT, 2015

107. This Act allows for the imposition of criminal sanctions for cybercrimes, which includes the misuse of technology, technological devices and/or digital data to cause economic/reputational loss or threaten physical injury or loss of life.

OTHER OFFENCES RELATING TO FRAUD, DISHONESTY AND CORRUPTION

108. 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 FSC Act, the BSA and the BOJA, the Credit Reporting Act, the Securities Act, the Insurance Act, the TCSPA and the Perjury Act.

SECTION III—INTERNATIONAL REGULATORY REQUIREMENTS

The United Nations (U.N. Convention against Transnational Organized Crime and the Protocols thereto, 2004 (Palermo Convention)

109. This established the following main obligations for member states of the U.N.:—

(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.

The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. 1988 (Vienna Convention)

110. This established the following main obligations for member states of the U.N.:—

(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 abovementioned 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.

The United Nations International Convention for the Suppression of the Financing of Terrorism, 1999

111. This established three main obligations for member states of the U.N.:—

(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.

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

The United Nations Resolution 1373, 2001

113. This Resolution identified threats to international peace and security caused by terrorist acts, also mandates all member states of the U.N. to take action against individuals, groups, organizations and their assets.

114. Because of the U.N.'s characterization of acts of terrorism as threats to international peace and security, the U.N. is entitled to take, if necessary, the collective measures (sanctions) under Chapter VII of the U.N.'s Charter. To this end, the Ministry of Foreign Affairs and Foreign Trade receives from time to time, an updated listing of individuals and entities which the U.N. has added to its consolidated list.

FATF Recommendations

115. In conjunction with these Guidelines, regulated businesses should be guided by the FATF standards, principles, best practices and recommendations in establishing policies, programmes and procedures to prevent and detect ML/TF/PF activities. The FATF Recommendations set out the internationally and regionally accepted principles relating to the appropriate measures to combat ML/TF/PF. The revised FATF Forty Recommendations can be accessed from both the FATF and CFATF websites at *www.fatf-gafi.org* and *www.cfatf.org*. 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 for the Life Insurance Sector, October 2018;

(d) Guidance for a Risk Based Approach for the Securities Sector, October 2018;

(e) Guidance on Proliferation Financing Risk Assessment and Mitigation, June 2021;

(f) Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, September 2020;

(g) Guidance on Digital ID, March 2020;

(h) Guidance for a Risk-Based Approach for Trust and Company Service Providers, June 2019.

Advisories and publications

116. Public statements and advisories in relation to high-risk jurisdictions are issued periodically by regional and international standard setting bodies and should be taken into consideration by regulated businesses when developing internal policies.

Advisories by FATF and CFATF

117. Public statements are issued on high-risk jurisdictions subject to a call for action and jurisdictions under increased monitoring. These are jurisdictions with significant AML/CFT deficiencies that have made insufficient progress in addressing these deficiencies, or which have not committed to an action plan developed with FATF/CFATF to address the deficiencies.

118. Public statements issued by FATF and CFATF can be accessed from their respective websites.

Advisory by the Financial Stability Board

119. According to the Financial Stability Board (FSB)[61], 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[62] (prepared by the IMF and World Bank) as well as signatory status to the multilateral MOU overseen by IOSC[63].

SECTION IV—RISK BASED FRAMEWORK

120. Under the FATF Forty (40) Recommendations, 2012[64]countries are required to identify, understand and assess the ML/TF risks posed to the country. Based on that assessment, countries must ensure that identified risks guide their national AML/CFT policies. This national risk assessment will therefore inform the overall national AML/CFT strategy and framework for a country and the implementation of appropriate risk-based measures for the relevant sectors within the country.

121. Jamaica conducted a National Risk Assessment ("NRA") the results of which were published in August 2021; included in the NRA are policy recommendations aimed at directing the deployment of resources to areas with the highest risks.

122. The NRA assessed the ML risks in nine (9) regulated sectors, including the life insurance and securities sectors. The life insurance sector was assessed as medium-low risk and the securities sector as medium risk. Jamaica's overall ML risk was medium-high risk.

123. The NRA also assessed other sectors that are currently not regulated for ML/TF such as: used car dealers, real estate developers, and the micro credit businesses (which are now regulated by the BOJ). An assessment was also conducted on TCSPs who have been recently brought under the AML/CFT/CPF regulatory framework and are now regulated by the FSC.

124. The main threats identified in the NRA were fraud (including advance fee fraud), trafficking in narcotics, trafficking in arms, and corruption. The major vulnerabilities of the country include a high crime rate, porous borders, its geographic location, deficiencies in the criminal investigatory and prosecution systems and the significant use of cash in the economy.

125. It is expected that regulated businesses will utilize the findings of the NRA to inform their own risk assessments of their customers, products and services.

126. The NRA can be accessed at *https://boj.org.jm/wp-content/uploads/2021/08/Public NRA Final 31 August 2021.pdf.*

RISK ASSESSMENT FRAMEWORK

Risk Management

127. The ML/TF risk of each regulated business is specific and requires an adequate risk management approach, which should correspond to the level and structure of the risk and the size of the business. The objectives of ML/TF risk management should enable a regulated business to establish a business strategy, risk appetite, adequate policies and procedures and promote high ethical and professional standards to prevent the business from being used for criminal activities.

128. ML/TF risk management requires the attention and participation of several business units with different competencies and responsibilities. It is important for each business unit to precisely know its role, level of authority and responsibility within the regulated business' organizational structure and within the structure of ML/TF risk management.

Role of Management

129. Management provides direction to operational activities by setting the risk appetite, formulating objectives and making strategic choices that form the basis for policies and procedures. Documentation and communication of strategy, and policies and procedures are therefore required. Management should ensure that adequate resources are allocated to risk mitigation and the implementation of satisfactory AML/CFT systems.

Risk Identification and Analysis

130. The first step in assessing ML/TF risks is to identify the risk categories, that is:

(a) Customers and other counterparts;

(b) Countries or geographic areas;

---

[61]FSB member countries—Australia, Argentina, Brazil, Canada, China, France, Germany, Hong Kong SAR, India, Indonesia, Italy, Japan, Korea, Mexico, The Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Switzerland, Turkey, United Kingdom and the United States of America.
[62]Report on Observance of Standards and Codes.
[63]International Organization of Securities Commissions.
[64]FATF Recommendation 1 and Interpretive Note to Recommendation 1.

(c) Products;

(d) Services;

(e) Transactions;

(f) Delivery channels; and

(g) Operating environment (business (size, activities and complexities); sector; national and global issues).

The significance of different risk categories will vary from one business to another.

131. A regulated business' risk assessment should be informed by the country's national risk assessment and 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).

132. For the analysis, a regulated business should assess the likelihood of the entity being misused for money laundering or terrorism financing. The likelihood will be high where, for instance, its customers are misusing the entity for ML on a frequent basis. In assessing the impact, the regulated business may conduct an evaluation of the financial impact of the crime itself and from regulatory sanctions; and the reputational damage that may incur.

Country or geographical Risk

133. Country or geographical risk may occur from the location of a customer or the origin or destination of a customer's transaction. However, the location of the organizational units of the business itself may constitute a higher level of risk. The factors that may indicate a higher risk include:

(a) Countries or geographic areas subject to sanctions, embargoes or comparable restrictive measures issued, by instance, by the United Nations;

(b) Countries or geographic areas identified by credible sources (for instance, FATF, IMF or the World Bank) as lacking an appropriate system of preventing ML/TF;

(c) Countries or geographic areas identified by credible sources as providing funding for or otherwise supporting terrorist activities;

(d) Countries or geographic areas identified by credible sources as having a high level of corruption, or other criminal activity.

Customer Risk

134. For its risk assessment, the regulated business should determine if a particular type of customer carries an increased level of ML/TF risk. Based on its own criteria, a regulated business can define the categories of customer that carries the most risk, which may include:

(a) Customers with frequent and unexplained transfer of funds to different institutions and frequent and unexplained movements of funds between accounts in various geographic locations;

(b) Customers where the structure or characteristics make it difficult to identify the true owner or controlling interests;

(c) Customers that use nominees, trusts, family members, third parties *etc*.;

(d) Cash intensive businesses including gas stations, supermarkets, used—car dealers, wholesales, gaming lounges etc.;

(e) Types of businesses identified in the NRA as high risk;

(f) Customers that are legal persons that are incorporated in offshore jurisdictions as international business corporations;

(g) Charities and other non-profit organizations;

(h) Indirect relationships through intermediaries who are unregulated;

(i) Politically Exposed Persons (PEPs); and

(j) Occasional customers that have transactions above a certain threshold.

Delivery Channels

135. The delivery channels should be included in any assessment of customer risk. The extent to which the regulated business has a direct relationship with customers, or through intermediaries or correspondent relationships, or establishes business relationships with non-resident customers are important factors in developing the risk assessment.

Transaction, Product and Service Risk

136. A comprehensive ML/TF risk assessment must take into consideration the potential risks from the transactions, products and services that the regulated business offers to its customers and the delivery channels of these products. Particular attention should be paid to risks arising from the application of new technologies. In identifying the risks of transactions, products and services, the following factors can be considered:

(a) Specialized services offered to high-net-worth persons (accredited investors);

(b) Services that offer anonymity or can readily cross international borders like wire transfers, online access to accounts *etc*.;

(c) New or innovative products or services that are not provided directly by the regulated business but are provided through its channels;

(d) Products that involve cash payments or receipt;

(e) One-off transactions; and

(f) Large single premium life insurance policies.

Risk Matrix

137. In conducting its AML/CFT risk analysis, the regulated business should establish whether all identified categories of risks pose a low, moderate, above average and high risk[65] to the business operations. The regulated business should review certain factors, e.g. the number and scope of transactions, geographical location, business type, whether cash or wire transfer is involved. The combination of these factors will indicate the level of ML/TF risk.

138. Regulated businesses can use a risk matrix as a method of assessing risk in order to identify the types or categories of customers that are low risk, those that carry higher but still acceptable risk and those that carry a high or unacceptable risk of money laundering or terrorism financing. The development of a risk matrix can take into consideration a wide range of risk categories, such as the products and services being offered, and the regulated business' size and organizational structure. A risk matrix is not static and should alter as the risk factors change.

139. The regulated business is to ensure that the risk identification and analysis is properly documented to demonstrate that this forms the basis of its AML/CFT policies and procedures. The FSC will also require sight of the risk assessment and the methodology utilized.

Policies and Procedures

140. The regulated business is required to document its policies and procedures with respect to its risk assessment and management processes. The policies and procedures should be approved by the Board and should be applicable to all business units, branches and majority-owned subsidiaries. They should allow for sharing of information between branches/subsidiaries with adequate safeguards on confidentiality and use of the information exchanged.

141. The policies and procedures should enable the regulated business to effectively manage and mitigate the identified risks and to focus its efforts on those areas that are more susceptible to ML/TF. The higher the risk, the higher the level of controls that are required.

Review of the ML/TF Risk Assessment

142. The risk assessment must be updated at least annually, or more frequently depending on the circumstances. This requires the regulated business to remain up to date with ML/TF methods and trends, international developments and changes in domestic legislation. A review should also be conducted when the business strategy or risk appetite changes or when deficiencies are detected in the effectiveness of the risk assessment.

RISK BASED APPROACH FOR AML/CFT SUPERVISORY ACTIVITIES

143. The FSC has adopted a risk-based approach in conducting its AML/CFT supervisory monitoring and enforcement activities. Effective supervision and enforcement are critical components of a robust AML/CFT regime. An effective supervisory and enforcement system comprises wide ranging financial supervisory measures that include preventative measures and related sanctions and other remedial actions.

144. This risk-based supervisory model takes into consideration several variables including:

(a) The size of the financial services sector;

(b) The complexity of the financial services sector;

(c) The degree of ML/TF risks;

(d) The level of compliance within the sector.

145. The FSC Utilizes a coordinated supervisory approach in its AML/CFT/CPF supervisory framework to construct a well-managed risk-based compliance programme. Where a regulated business forms part of a financial group, the FSC's responsibility for supervising and enforcing the AML/CFT/CPF compliance of the said business is shared with other relevant competent authorities.

146. The FSC continues to apply the Core Principles established by global standard setting bodies[66] for effective supervision and regulation by competent authorities. Under these Core Principles, effective supervision is:

(a) risk-based, focusing on both major prudential and conduct of business risks, as well as a wide range of other risks, such as compliance risk, reputational risk, legal risks and ML/TF risks;

(b) the result of a combination of off-site and on-site supervision;

(c) based on having appropriate access to all the books and records of each regulated business sufficient to collect the widest range of information that a supervisor needs; and

(d) inclusive of the international element of a regulated business or groups operating across borders by allowing for international cooperation.

147. In assessing the effectiveness of the FSC's AML/CFT/CPF supervisory regime, the following factors will be considered:

(a) The successful exclusion of criminals and their associates from holding or being the beneficial owner of a significant interest or holding a management function in a regulated business. This exclusion relies on licensing, registration or other controls (like fit and proper checks) that have been implemented;

---

[65]Businesses may also use a three-tiered risk level (i.e. low, medium and high).
[66]Some of which include IOSCO, IAS and IOPS.

(b) The ability to identify and maintain an understanding of the ML/TF risks in the financial and other sectors as a whole, between different sectors and types of institution, and of individual institutions;

(c) The ability, on a risk sensitive basis, to supervise or monitor the extent to which regulated businesses are complying with their AML/CFT requirements with a view to mitigate the risks;

(d) The extent to which remedial actions and/or effective, proportionate and dissuasive sanctions are applied;

(e) The extent to which the FSC is able to demonstrate that its actions have an effect on compliance by regulated businesses;

(f) The extent to which the FSC promotes a clear understanding to regulated businesses of their AML/CFT obligations and ML/TF risks.

Risk Profile

148. The FSC has developed a four-tiered risk profile for all its regulated entities.

TABLE 4—TIERED RISK PROFILE

Risk Profile	Rating
Low	1
Moderate	2
Above Average	3
High	4

149. The risk profile of a regulated business is developed using a combination of information from onsite inspections, responses from the self-assessment questionnaire, interviews, the level of high risk customers, the level of foreign currency transactions, the level of high risk products, acceptance of cash transactions, adverse information from another Competent Authority, the Designated Authority or law enforcement, ownership or management by a PEP and adverse business conduct derived from the prudential audit.

150. The risk profiles of each regulated business are updated annually. The frequency of onsite inspections will be influenced by the risk profile of a regulated entity, where there will be more frequent onsite visits for entities that are rated as high risk.

Supervisory Examination Framework

151. The FSC's AML/CFT/CPF supervisory examination framework includes the following:

(a) Clear and adequate methodologies and procedures for both off-site supervision and on-site inspections.

(b) Off-site monitoring tools include questionnaires on the policies, procedures, and reporting systems in place at regulated businesses.

(c) On-site assessment tools include assessing the adequacy of AML/CFT controls, such as management reporting and oversight.

(d) risk-based assessments conducted across all or part of a financial sector using a thematic approach (thematic studies).

(e) an inspection or review of a regulated business' governance and controls over third-party service providers where AML/CFT/CPF activities are outsourced. This is to establish whether the regulated business' arrangements comply with its AML/CFT/CPF obligations.

SUPERVISORY TOOLS

152. The FSC's examination process includes an assessment of the adequacy of a regulated business' AML/CFT/CPF policies and systems, the institution's compliance with these policies and systems as well as the applicable legislation and the Guidelines. Accordingly, the AML/CFT/CPF oversight of regulated businesses by the FSC is to—

(a) assist with understanding each regulated business AML/CFT/CPF risks;

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

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

Off-site Monitoring

153. The major off-site monitoring tool utilized by the FSC is a self-assessment questionnaire that is sent to regulated businesses periodically. The data garnered from the completed questionnaire is processed, analysed, and used to update the risk profile of each regulated entity. This questionnaire is updated annually to ensure its relevance and usefulness.

154. Other off-site monitoring tools that are being deployed by the FSC are:

(a) Thematic reviews;

(b) Desk based reviews;

(c) Meetings and interviews with the Nominated Officer and other relevant staff; and

(d) Reviews of internal and external AML/CFT/CPF Audit Reports.

On-site Monitoring

155. On-site AML/CFT audits may take one of the following forms:

(a) full scope examination;

(b) targeted examination;

(c) thematic examination.

156. An on-site examination may be conducted based on any of the following reasons:

(a) the risk profile of the regulated business;

(b) a regularly scheduled examination;

(c) a request by another Competent Authority;

(d) a request from the Designated Authority; or

(e) receipt of adverse information.

157. Regulated businesses should be aware that as the Competent Authority, the FSC could 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 regulated business' breach of its obligations under the applicable legislation can, in addition to the imposition of sanctions, also be reported to the Designated Authority.

SECTION V—CUSTOMER DUE DILIGENCE (CDD), KNOW YOUR CUSTOMER ("KYC")

Interpretation

For the purpose of this section—

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

"business classification" is as follows:

Category	No. of Employees
Small	Up to 20
Medium	21–50
Large	Over 50

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

"known employer" includes:—

(a) in the case of a business, one that is registered on the Jamaica Stock Exchange; or a micro, small or medium enterprise (MSME) that is either licensed to operate or, if no such regime exists, one which is required to be registered with a government body or agency or statutory body pursuant in order to operate and is so registered;

(b) in the case of a business, one that is a customer of the regulated business for a period of not less than ten (10) years;

(c) a financial institution as defined in the Guidelines; or

(d) an employer within the public sector. Public sector for the purposes of the Guidelines means the Central Government or a public body as defined in the Financial Administration and Audit Act.

"longstanding customer" means a customer with which:

(a) a business relationship is held with the financial institution and 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 and the customer is not high risk.

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

"*on-going 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.

"*out-dated information*"	refers to information regarding the personal, business or official affairs of the customer, that includes:— (a) expired identification; (b) a change of name of the customer; (c) change in customer's residential address, (in the case of a natural person); (d) change in customer's registered address (in the case of a legal person); (e) financial statements which have not been updated for 18 months or more; (f) any information in respect of which an intervening event has occurred, which makes the information provided, unreliable or unhelpful for the institution to undertake its know your customer and customer due diligence and risk profile analyses.
"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(l)(c) of the POC (MLP) Regulations and at regulation 13(l)(c) of the TP (Reporting Entities) Regulations.
"public body"	means a statutory body or authority or any government company (section 2—The Financial Administration and Audit Act).
"records"	includes records pertaining to identification, transactions, business correspondence, account files, instructions, reasons 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.
"regulated entity or business"	refers to entities regulated by the FSC.
"repeat customer"	means a person who transacts business of a minimum of US$250 or its equivalent with the regulated business and any of its subsidiaries or other connected parties or affiliates more than once within a three-month period.
"senior officer"	in relation to a body corporate or any other legal arrangement, 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 or has responsibilities akin to these positions.
"significant transaction"	means a transaction undertaken by a regulated business in respect of a customer, which varies substantially in value and/or volume 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 investment activities for a corporate customer is used to finance or cover personal expenses; or (c) substantial increase in deposits to the savings/investment portion of an insurance policy.

GENERAL REQUIREMENTS FOR KNOW YOUR CUSTOMER ("KYC AND CUSTOMER DUE DILIGENCE ("CDD")

158. General CDD[67] requirements involve the obligation to know your customer by satisfactorily identifying the customer, verifying their identity and establishing details pertaining to the customer's:

(a) occupation and economic activity;

(b) personal financial information and the historical financial performance of the business;

[67]Regulations 7, 11, 12 and 13, POC-MLPR; Regulations 7, 11, 12 and 13, TP-RER; and FATF Recommendation 10.

(c) source of funds ("SOF") and/or source of wealth ("SOW");

(d) contact information;

(e) capacity in which the business is being transacted and details of representation relationship, authorities established to act for persons benefiting from the transaction or relationship with the regulated business;

(f) regulatory compliance status (e.g. tax compliance record, professional association standing);

(g) criminal background[68] (e.g. via open-source searches).

159. In the case of customers that 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[69]. The CDD must enable a regulated business to know its customer by obtaining information on what the customer does and why that customer requires the services requested of the regulated business.

160. As soon as is practicable, but no later than 14 days after contact is made between a regulated business and an applicant for business concerning any business relationship or one-off transaction, the following obligations come into effect:

(a) The applicant for business produces satisfactory reliable evidence of his identity to the regulated business;

(b) The regulated business takes the required measures to verify the applicant's identity; and

(c) Risk management measures are applied to the conditions under which the business relationship or one-off transaction is dealt with, while identification procedures to verify the applicant's identity are being carried out.

161. Risk management measures may include the following:

(a) Restricting the number of transactions that are conducted on the account;

(b) Restricting the types of transactions that are allowed (for instance, precluding wire transfers and/or foreign currency transactions); and

(c) Applying a threshold on the value/size of transactions.

162. Where the regulated business is unable to verify the applicant's identity within fourteen (14) days after contact is first made, the regulated business must then act as set out below:

(a) Where a regulated business is not satisfied with the outcome of its CDD inquiries, but there are no reasonable grounds to suspect that the business relationship or one-off transaction constitutes or could be related ML, then:

(i) The business relationship or one-off transaction must be terminated unless conducted with the permission of, and in accordance with guidelines issued by, the FSC; and

(ii) The regulated business shall make an assessment as to whether any disclosure is required under section 94 or 95 of the POCA; that is, a suspicious transaction report ("STR");

(b) Where the regulated business has reasonable grounds to suspect that a business relationship or one-off transaction constitutes or could be related to ML and is of the belief that carrying out the full required CDD measures might alert the person that such a suspicion has been formed, then the regulated business should act as follows:

(i) Discontinue the CDD procedures;

(ii) Make the required disclosure (STR) under section 94 or 95 of the POCA or section 16(3) of the TPA;

(iii) ensure that in discontinuing the CDD procedures, it has collected enough information to adequately identify the applicant so that it can submit a valid STR[70] to the FID.

163. A regulated entity undertaking verification, should establish to its reasonable satisfaction that every verification subject, relevant to the application for business, exists. Where there may be a large number of verification subjects, (in multiple-owned accounts/businesses) it may be sufficient to carry out verification on a limited group only, such as the senior members of the family, the principal shareholders, the main directors of the company, *etc*.

164. A regulated entity should carry out verification in respect of the parties operating the account. However, where there are underlying principals, the true nature of the relationship between the principals and the account signatories must also be established. Appropriate enquiries should be performed on the principals, especially if the signatories are accustomed to acting on their instructions. In this context "principals" should be understood in its widest sense to include, for example, beneficial owners, settlors, controlling shareholders, directors, major beneficiaries, but the standard of due diligence will depend on the exact nature of the relationship.

165. Regulated businesses are prohibited from keeping anonymous accounts, fictitious names or numbered accounts.

166. Where an applicant for business refuses to produce any requested information, the relationship or the transaction should not proceed. Where an existing customer unreasonably refuses to provide the information requested by the regulated business pursuant to CDD/ KYC requirements, or if any other verification problems arise which cannot be resolved, the business relationship with that customer must be terminated (unless otherwise advised by law enforcement authorities). Nevertheless, special consideration should be given for long term life insurance contracts based on the nature of such contracts and the effect of the termination of same.

---

[68]This is not a requirement to obtain a police record/report.
[69]FATF Recommendation 10.
[70]The FID's reportng portal, goAML has established minimum standards for the acceptance of a report from a reporting entity. Therefore, any report submitted that does not have specified mandatory information will be automatically rejected by the portal.

167. In seeking to discontinue the procedures for establishing a business relationship or a transaction started or attempted; or terminate the business relationship, regulated businesses should be mindful of the prohibition against tipping off or unauthorised disclosures outlined under sections 97 and 104 of POCA, section 17 of the TPA and section 5(6) of the UNSCRIA. Regulated businesses should therefore be careful not to "tip off" applicants for business, customers, or any other person where a suspicion has been formed by the regulated business that an offence is being attempted or has been or is being committed.

168. Regulated businesses should ensure that they have the ability to legally terminate arrangements, transactions or the business relationship, where they 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.

169. Prior to termination of a business relationship, where there is suspicion that funds in an account may constitute criminal property, regulated businesses should seek appropriate consent from the Designated Authority before returning such funds to the customer.

Updating Customer Information

170. Regulated businesses should undertake regular reviews[71] of all existing customers' records (identification and other particulars) to ensure that they remain up-to-date, relevant, consistent with the risk profile of that customer, and remain subject to appropriate CDD and EDD processes. These reviews should be done at least seven (7) years from the date of the commencement of the relationship and at minimum, seven (7) year increments thereafter, or at more frequent intervals as warranted by the risk profile to ensure the accuracy of the information held by the institution.

171. The agreement with the customer should place an obligation on the customer to notify the regulated business 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 regulated business to be out-dated.

172. Reviews[72] should 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 the customer's transactions are inconsistent with his financial profile;

(e) When, during the course of the business relationship, doubt arises regarding the identity of the customer or the beneficial owner of the account;

(f) When there is any change in the ownership or control of a corporate customer, or of a customer established through a legal arrangement;

(g) Where the regulated business becomes aware at any time that it lacks sufficient information about an existing customer/or about the existing business relationship with a customer;

(h) Where any cash transaction involves/exceeds the prescribed amount and represents a significant transaction, or a material change in the manner in which the account is operated[73];

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

(j) Where there are concerns or inconsistencies surrounding a transaction that is carried out by means of wire transfer;

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

(l) Where the regulated business is required to make a report under section 94 or 95 of the POCA, or under section 16(3) of the TPA (STR).

173. If, during the course of conducting ongoing CDD, a regulated business discovers that the information on file is inaccurate and cannot be updated; or is unreasonably withheld, it must take steps to terminate the relationship[74] and consider whether it should file an STR.

174. Where there are gaps in the KYC database[75] regulated businesses must ensure that the requisite information is obtained promptly and not at the end of a seven (7) year period from the last update. Updates in this regard would include matters involving—

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

(b) incomplete information—for instance, the customer provided an alias or trading name other than the customer's name as defined in the Guidelines, then the information on the institution's records 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; and identification updates. Regulated businesses should ensure that the records reflect the current information;

---

[71] Regulations 7, 7A and 19, POC-MLPR, Regulations 5, 5A and 21, TP-RER.
[72] Regulations 7(1)(c), 7(3) and 7A(5)(c), POC-MLPR; Regulations 5 and 6(2)(b), TP-RER
[73] POCA speaks to the following prescribed amounts—a TTR limit for cash transactions (see Regulation 3, POC-MLPR) and cash transaction limits (see section 101A, POCA).
[74] Regulation 7(l)(b), POC-MLPR and Regulation 5(a)(iii), TP-RER.
[75] The law indicates that for accounts that pre-date the prescribed date of 29th day of March 2007, only identity updates (which includes address verification) are required (see Regulation 19, POC-MLPR). **This exclusion clause does not apply to high-risk accounts**.

(d) correcting errors or addressing inaccuracies.

Natural Persons

175. Identification must be obtained from documents issued by reputable sources that may include any one of the following:

(a) valid driver's licence, issued by the authorities in the country in which the person is resident;

(b) valid passport;

(c) valid voter's identification card;

(d) Current Known Employer or Public Sector Employer Identification Card (with a photograph, signed by both the employee and employer and which has an expiry date).

176. In cases where the identification described above genuinely cannot be produced, the regulated business will need to determine whether it should allow the use of alternative forms of identification in circumstances where the customer is low-risk (See SDD below).

177. The acceptable forms of alternative identification include, in the case of:—

(a) an applicant for business, a birth certificate accompanied with a Voluntary Declaration of Identification from a person who is personally known to and who has a familial relationship with the applicant for business (i.e. parent, guardian or older sibling etc.), and a photograph. Both the Declaration and the photograph must be signed by any one of the following persons to whom the customer shall be personally known for a period of not less than twelve (12) months, and who can confirm the identity of the customer:

(i) Justice of the Peace (JP);

(ii) Notary Public;

(iii) Member of the judiciary;

(iv) Attorney-at-Law; or

(v) Jamaica Constabulary Force Officer (at the rank of Superintendent and above);

(b) a customer or applicant for business who has not attained the age of majority (18 years), and who is enrolled in a secondary or tertiary institution, a valid school ID may be accepted provided that:

(i) The ID has the following features:

- A photograph of the student;
- Signature of ID holder (student);
- ID Number;
- Expiry date of ID;
- Name of the relevant academic institution (high/secondary school or tertiary institution);
- Signature of principal/vice-principal/bursar of the relevant academic institution; 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 who is either the parent or legal guardian of the customer.

178. Where a regulated business is approached for business by a person seeking to use an acceptable form of alternative identification, the regulated business must ensure that appropriate safeguards in place are consistent with the assessed risk profile of the customer such as, transaction threshold limits applied to the business transacted.

179. In cases where documentary evidence of identity and independent verification of address of vulnerable customer[76]cannot be produced, a senior member of key staff may authorize the opening of an account if he is satisfied with the circumstances and should record these circumstances in the same manner and for the same period as the identification records. If the verification subject is an existing customer of an institution acting as an intermediary in the application, the name and address of that institution and that institution's personal reference on the verification subject should be recorded.

180. A regulated business that relies significantly on an acceptable alternative form of identification outside of the parameters indicated above, will be deemed to be acting contrary to its KYC/CDD obligations and will expose itself to regulatory action.

181. The policies and procedures should clearly indicate the transaction safeguards and other measures that will be applied to minimize the risk of conducting business with a person using an alternative form of identification.

182. The following information is required to satisfy basic CDD requirements for natural persons and any customer information order served on the financial institution[77]:—

(a) Customer Identification Information;

(b) Account/transaction number;

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

---

[76] Persons who are normally excluded from the financial sector due to their particular circumstances.

[77] Section 120(2) and (3), POCA; Regulation 7(5), POC-MLPR (where customer information is defined and same includes the TRN); or Regulation 13(1)(c), POC-MLPR (other relevant reference number and the identity of the settler and beneficiary in arrangements involving settlements or trusts).

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

(e) Transaction date and description of transaction type;

(f) Details of any other accounts to which the individual is a signatory (including the account number and the personal or private information of the holders of 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) Occupation or economic activity generating the source of income;

(i) Business and personal contact details;

(j) Capacity in which the business is being transacted (such as details of the representative relationship);

(k) Information regarding the customer's character and integrity (except for customers who are visitors to the island and not transacting business in the course of, or pursuant to a work permit situation);

(l) 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)

183. The following information[78] must be obtained from all prospective customers:

(a) Full true name and other names/aliases used;

(b) Current permanent address, including postal address (if different from the permanent address);

(c) Date of birth;

(d) Place of birth;

(e) Nationality;

(f) Mother's maiden name;

(g) Taxpayer Registration Number (TRN) (or other national reference number);

(h) At least two (2) references for customers (except for occasional customers who are visitors to the island and not transacting business in the course of, or pursuant to a work permit situation);

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

(j) Employment/occupation/business activity; and

(k) SOF and/or SOW.

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

184. Under the POC-MLPR, customer information includes the TRN or other reference number. The FSC advises that this 'other reference' number means a national number issued in another jurisdiction e.g. Social Security Number (SSN), in the case of the United States of America.

Address Verification Documents

185. The current permanent address of the applicant for business should be verified by an independent and reliable source. The following methods may be used[79]:

(a) Utility Bill;

(b) Telephone Directory;

(c) Voter Identification Card;

(d) Credit Card Statement or Bank Statement (issued by mail by another financial institution);

(e) Letter from a Justice of the Peace (JP) or Notary Public;

(f) Driver's Licence;

(g) Confirmation from a "Trusted Referee";

(h) Official letter issued by a government agency/authority;

(i) Letter from Known Employer or Public Sector Employer.

RESTRICTION ON USE OF SAME DOCUMENT FOR DUAL PURPOSES

186. A regulated business may not use the same document for both proof of identification and proof of address. Therefore, if for example, a driver's licence is provided for identification purposes, then another document should be used to verify the address of the applicant for business. This restriction serves to provide further safeguards in the verification of customer identification information.

---

[78] Regulation 7, POC-MLPR; and, where applicable, the information referred to, at Regulation 13(1)(c), TP-RER, (i.e. identity of beneficial owner).
[79] See methods of validating of documents used for verification purposes.

Verification of CDD and Transaction Details

187. The name, permanent address and employment/business details of a customer should be verified by independent and reliable sources and validated (as necessary) by original documents, as follows:

(a) a utility bill with its date not past three (3) months, for example, electricity, telephone, water, cable and internet:

(i) in the name of the customer; or

(ii) in the case of an applicant for business who is a minor and/or is a student, in the name of the parent/guardian of said applicant for business;

(b) a local telephone directory;

(c) a current stamped lease agreement;

(d) identification card issued by the Electoral Office of Jamaica;

(e) Credit Card Statement or Bank Statement—original statement issued by another financial institution and mailed to the customer with its date not past three (3) months;

(f) Official letter issued by a government agency/authority and mailed to the customer with its date not past three (3) months;

(g) Letter from a Justice of the Peace (JP) or Notary Public where:

(i) the referenced individual is personally known[80] to the JP or Notary Public; and

(ii) the JP/Notary Public can confirm that the address is the referenced individual's true place of residence;

(h) Driver's licence issued by an authorised government agency;

(i) Confirmation from a "Trusted Referee" who is:

(i) a person known to the applicant for business, for a minimum period to be determined by the regulated business, based on its risk assessment of the applicant;

(ii) a person who is not involved in the transaction being engaged in by the applicant for business; and

(iii) a person on whom the regulated business places reliance.

(j) Letter from Employer—where the Applicant for Business is employed to a known employer or an employer within the public sector, then the Applicant's Employer can:

(i) issue an address verification letter;

(ii) confirm employee identification cards;

(iii) confirm customer's details and status of employment independently; and/or

(iv) confirm customer's salary and benefits.

(k) Passports issued by an authorised government agency;

(l) Cross-checking KYC details with other regulated 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 which the funds were sent). In so doing, regulated businesses will need to be guided by the respective Agreements with the customer that should ideally reflect that the customer's consent has been obtained to do this type of check.

(m) Cross-checking KYC details provided with other affiliated companies within the corporate group with whom the customer has also done business.

(NB. Reference to the customer also includes reference to the applicant for business)

188. Verification is a cumulative process; it is not appropriate to rely on any single piece of documentary evidence. The best possible documentation of identification should be required and obtained from the verification subject. For this purpose, "best possible" means that which is the most difficult to replicate or acquire unlawfully because of its reputable and/or official origin.

SELF-EMPLOYED PERSONS AND SOLE PROPRIETORS

189. Regulated businesses 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 as outlined under "Natural Persons" 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);

---

[80] For a minimum period of 12 months.

(d) A financial statement of the business;

(e) Documentation listed at (j), (l) and (m) as outlined in the Bodies Corporate section below.

190. 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

191. Regulated businesses should be vigilant when dealing with corporate vehicles as they may be used as a method of securing anonymity. *In all cases, the regulated businesses*[81] *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*.[82] This applies to both local and overseas corporate clients. Regulated businesses shall 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 in accordance with the customer's risk profile or when conducting significant transactions for existing bodies corporate:

(a) Certificate of Incorporation or certificate of registration;

(b) Articles of Incorporation;

(c) Directors' Resolution authorizing company's management to engage in transactions;

(d) Instructions to the regulated business, signed application form, or an account opening authority containing specimen signatures;

(e) Audited financial statements of the business, 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);

(f) the most recent annual return filed with the Registrar, duly notarized where such corporate body is incorporated outside Jamaica;

(g) a list of names, addresses and nationalities of principal owners, directors, beneficiaries, and senior management as well as any person with authority to sign off on contractual arrangements;

(h) copies of identification documents should be obtained from each director; each shareholder holding 10% or more of voting rights or ownership of the company, and authorized signatories in accordance with the general procedure for the verification of the identity of individuals;

(i) certified copies of Powers of Attorney or other authorities given by the directors in relation to the company;

(j) 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);

(k) Group/Corporate structure, where applicable;

(l) 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);

(m) Tax Compliance Certificate (TCC)[83] or other equivalent official confirmation from the relevant tax authorities of compliance with income tax obligations;

(n) The source of wealth of the corporate customer and the source of funds being placed with the regulated business and the purpose of the account;

(o) A business plan indicating the projected turnover or volume of activity in the account.

Verification of the information provided on the directors and beneficial owners

192. 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.[84] Disclosures on the particulars of owners, and directors must include disclosures in relation to nominee shareholders and nominee directors and shadow directors[85].

193. 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.[86]

---

[81] Regulations 11, 12 and 13, POC-MLPR.
[82] Ibid
[83] 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.
[84] Regulation 13(1)(c)(iii), POC-MLPR;
[85] As defined in the Companies Act.
[86] Regulations 13(1)(c)(i)(A) and 13(1)(c)(ii)(B), POC-MLPR; Regulation 13(1)(c)(i)(A), TP-RER.

194. 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.

Listed Companies

195. Pursuant to the 2019 amendments to the POC-MLPR, companies listed on the Jamaica Stock Exchange (JAMSTOCK) are no longer exempted from CDD identification and verification measures. Identification and verification procedures as stated above are applicable to listed companies. Notwithstanding the requirement to identify persons holding ten per cent (10%) or more of the voting rights/shares in a listed company, a variation of the CDD treatment is necessary due to the following:

(a) Some amount of due diligence would already have been conducted on shareholders; and

(b) The constant changing of the shareholdings due to daily trading on the stock exchange.

196. The identification and verification of shareholders owning 10% or more of a listed company should be conducted as follows:

(a) At on-boarding, the application of CDD and EDD, as applicable; and

(b) Annual identification updates, using data from the JAMSTOCK website.

197. Where there are no shareholders owning 10% or more of shares, regulated businesses are to conduct CDD/EDD on the beneficial owners.

198. Beneficial ownership identification and verification requirements are to be enforced in any case.

PARTNERSHIPS

199. Regulated businesses should fully understand the obligations, responsibilities and entitlements arising under the partnership[87], the source of wealth accumulated by the partnership, the source of funds involved in the transaction and the controllers and beneficiaries thereunder. This should be the case whether the partnership is locally established or established overseas. Regulated businesses should also ensure that they obtain the following information and documents or their equivalents in respect of new accounts and undertake appropriate reviews of such information and documentation when conducting significant transactions involving partnerships or similar arrangements—

(a) Partnership Deed;

(b) Business registration certificate;

(c) The authority to undertake or agree to engage in transactions which legally bind the partnership;

(d) Signing authority for the account mandate and specimen signatures;

(e) 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

(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;

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

(g) 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 regulated business or on request;

(h) 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, TRN, business or registered address of the affiliated entity and the nature of the relationship with the affiliated entity;

(i) TCC or other equivalent official confirmation from the relevant tax authorities of compliance with income tax obligations;

(j) Confirmation of the source of funds being placed with the regulated business and source of wealth of the partnership for high-risk customers.

---

[87] The Partnership (General) Act and Partnership (Limited) Act were passed in January 2017 but are not yet in effect. These pieces of legislation allow the partnership to have a separate liability from its owners.

PRINCIPALS AND BENEFICIAL OWNERS UNDER TRUSTS, SETTLEMENTS AND OTHER LEGAL ARRANGEMENTS[88]

200. Regulated Businesses should ensure that they obtain the following information and documents or their equivalents in respect of new accounts and 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[89] 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 Records Office (of the Registrar General's Department);[90]

(b) Identification, verification, and other details outlined for Natural Persons above are equally applicable in relation to all principals of trusts (trustees, settlors, beneficiaries, enforcers (if any), protectors), 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[91]. Verification of identification information provided on such principals and beneficial owners should be independently verified from the Island Records Office (of the Registrar General's Department, where applicable). Otherwise, ownership and director identification details should, at a minimum be accessible from the trustee for the trust or other legal arrangement, or from the trust or corporate service provider, on the authorisation of the trustee.[92]

CHARITIES

201. Special care should be taken by regulated businesses in dealing with unincorporated bodies (such as foundations, associations etc.) 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.

202. Regulated businesses 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 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 that have been established as bodies corporate, the information set out above under Bodies Corporate;

(e) List of names, addresses and nationalities of principal owners or of the beneficial owners (if different from the principal owners) or the individuals who ultimately 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 be 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;

(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). Regulated businesses will need to ascertain whether the information provided by the charity is sufficient to allow for a determination to be made by the regulated business regarding the risks of doing business with the entity.

(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.

---

[88] Regulations 11,12 and 13, POC-MLPR.
[89] Trusts Act.
[90] Section 10(6), Trusts Act.
[91] Regulation 13(l)(c)(i)A, POC-MLPR; Regulation 13(1)(c)(i)A, TP-RER.
[92] Regulation 13(l)(c)(ii)(B), POC-MLPR.

CLUBS AND SOCIETIES

203. In the case of accounts being opened for clubs and societies, the regulated business should satisfy itself as to the legitimate purpose of the organization by, for example, requesting a copy of the constitution and certificates from the Companies Office of Jamaica, the Department of Cooperative and Friendly Societies and any other relevant authority. This should include verification checks with the relevant authorities. Where there is more than one signatory to the account, the identity of at least two signatories should be verified initially and, when signatories change, care should be taken to ensure that the identity of at least two current signatories have been verified.

CUSTOMERS RESIDENT OVERSEAS

204. Regulated businesses should apply equally effective customer identification procedures and on-going monitoring standards to non-resident customers. Based on the inherent risks for these accounts, and the designation of these accounts as high risk[93], Enhanced Due Diligence (EDD) measures should be applied.

205. Even though both resident and non-resident customers can provide the same documents, there is a greater difficulty in matching the customer with the documentation in the case of non-resident customers. In accepting business from non-resident customers, regulated businesses should have specific and adequate measures to mitigate the higher risk. These measures, in addition to applicable EDD measures may include:

(a) certification of documents presented;

(b) requisition of additional documents; and

(c) independent verification of documents by contacting third party.

206. Regulated businesses are required to ensure that, among other things, its AML/CFT/CPF 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.[94] For the purposes of these Guidelines, the jurisdictions targeted for this special attention include jurisdictions flagged by:

(a) FATF;

(b) UNSC;

(c) A country with which Jamaica is Party to a treaty that requires either Party to take certain actions in relation to nationals of either country in accordance with the circumstances outlined in such treaty; and

(d) *Gazette*—Notice of Designation of Specified Territories (November 23, 2021).

207. Regulated businesses should exercise a high level of caution when establishing business relationships with foreign companies that have nominee shareholders or bearer shares. If the ultimate beneficiaries or beneficial shareholders 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.

208. Regulated businesses should exercise particular care when dealing with overseas counterparties, or businesses acting for overseas clients, where to the local institution's knowledge, the overseas counter-party or representative business is not subject to AML/CFT/CPF 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, regulated businesses should carefully scrutinize any proposed transaction with any client, counter-party or financial institution situated in a jurisdiction with weak or non-existent AML/CFT/CPF 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. Regulated businesses should also be alert to any mitigating actions taken by such jurisdictions to effectively deal with such matters.

NON-FACE-TO-FACE CUSTOMERS/ DIGITAL ONBOARDING OF CUSTOMERS[95]

209. In the opening of new accounts with non-face-to-face customers, the regulated business needs to implement digital identification ("ID") systems that meet the required assurance threshold for identity proofing and authentication. The institution should ensure that it has the appropriate technology and has implemented adequate organizational and governance standards to provide trustworthy, secure, private and convenient avenues for identification and verification of the identity of applicants for business.

210. The advantages of utilising reliable digital onboarding systems include:

(a) improved processes for customer identification and verification at onboarding;

(b) on-going due diligence and scrutiny of transactions throughout the course of the business relationship; and

(c) reduced costs and increased efficiencies in the onboarding process.

211. Potential risks in the utilisation of digital onboarding systems include: cyber security, identity theft, fraud and ML/TF.

212. The implemented digital ID system should have at minimum the two basic components set out below.

---

[93] Regulation 7A(2), POC-MLPR.
[94] Section 94A, POCA.
[95] See FATF's Guidance on Digital Identity.

Component One: Identity Proofing and Enrolment

213. This component involves the collecting, validating and verifying the identity of the applicant for business; establishing an identity account (enrolment) and binding the person's unique identity to authenticators in the possession and control of this person.

214. The steps taken in Component One would include:

(a) Collection: Collect identity attributes online such as the completion of an online application form, capturing a photo of the applicant, uploading IDs such as a driver's licence or passport, address and income verification documents and other CDD documents;

(b) Validation: Reviewing of documents to ensure authenticity and accuracy of data such as date of birth, expiration dates and checking with issuing authorities such as Tax Administration Jamaica;

(c) De-duplication: establish that the identity attributes and evidence relate to a unique person;

(d) Verification: link the individual to the identity evidence provided (for instance, by the use of biometric solutions, such as facial recognition and liveness detection);

(e) Enrolment in identity account and binding: Create the identity account and issue and link one or more authenticators with the identity account (e.g. passwords, one time code (OTC) generator).

Component Two: Authentication and Identity Lifecycle Management

215. Authentication establishes that the person who has been identified and verified is the same person having possession and control of the authenticators. There are three types of factors for the authentication of the customer:

(a) Ownership factors (card, mobile app, certificate, security token, access badge);

(b) Knowledge factors (password); and

(c) Inherent factors (biometrics).

216. A single authentication factor is not sufficiently trustworthy. For an authentication process to be robust and reliable it must utilise multiple types of authentication factors. A regulated business may consider other authentication factors such as log-in channels, geolocation, frequency of usage, type of usage and IP addresses.

217. Identity lifecycle management refers to the responses to events that occur over the identity lifecycle and affect the use, security, and trustworthiness of authenticators. Some of these events are loss, theft, unauthorised duplication, expiration and revocation of authenticators and/or credentials.

218. Digital onboarding systems do not inherently attract higher level of risks than routine face-to-face onboarding since any such system that operates at the required assurance threshold facilitates more effective validation/verification processes for CDD information.

TRANSACTION COUNTERPARTIES

219. A counterparty to any transaction with a regulated business shall be subject to the same due diligence undertaken in relation to customers, as far as this is applicable in the circumstances.

VERIFICATION OF IDENTIFICATION DETAILS POST-COMMENCEMENT OF BUSINESS

220. As soon as is reasonably practicable, but no later than fourteen (14) days after contact[96] is made between a regulated business and an applicant for business concerning any business relationship or one-off transaction, the following obligations come into effect:

(a) The applicant for business produces satisfactory reliable evidence of his identity;

(b) The regulated business takes the required measures to verify the applicant's identity; and

(c) Risk management measures are applied to the conditions under which the business relationship or one-off transaction is dealt with, while identification procedures to verify the applicant's identity are being carried out.

221. Risk management procedures may include the following:

(a) Restricting the number of transactions that are conducted on the account;

(b) Restricting the type of transactions that are allowed (for instance, precluding wire transfers and/or foreign currency transactions); and

(c) Applying a threshold on the value/size of transactions.

222. Where a regulated business is not satisfied with the outcome of its CDD inquiries, but there are no reasonable grounds to suspect that the business relationship or one-off transaction constitutes or could be related to ML then:

(a) The business relationship or one-off transaction must be terminated unless conducted with the permission of, and in accordance with guidelines issued by the FSC; and

(b) The regulated business must make an assessment as to whether any disclosure is required under section 94 or 95 of POCA.

---

[96] Regulation 7, POC-MLPR.

223. Where a regulated business has reasonable grounds to suspect that a business relationship or one-off transaction constitutes or could be related to ML and is of the belief that carrying out the full required CDD measures might alert the person that such a suspicion has been formed, then the regulated business should:

(a) Discontinue the CDD procedures; and

(b) Make the required disclosure (STR) under section 94/95 of POCA or section 16(3) of the TPA.

224. The regulated business has to ensure that in discontinuing the CDD procedures, it has collected enough information to adequately identify the applicant so that it can submit a valid[97] STR to the FID.

CONFIRMATION OF KYC/CDD WITH THE ASSISTANCE OF OTHER REGULATED BUSINESSES

225. In some cases, a regulated business may require the customer to issue instructions to another regulated business with whom the customer has dealings, and which institution is able to provide appropriate KYC verification for the customer in question. It is recommended that regulated businesses enter into written arrangements to facilitate information sharing within the parameters of the law. Where KYC/CDD verification is pursued through this option and the information is still not forthcoming:

(a) the transaction should not proceed;

(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.

226. 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/CDD information.

TRANSACTION VERIFICATION

227. Transaction verification involves ensuring that the transaction indicated and conducted is the one intended by the customer/counterparty. The verification processes may 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.

(b) That transactions indicated are the actual 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. For instance, transactions in which the payment is not directly reflected between the entity and the counterparty, should be flagged.

228. Under the POC-MLPR, a record of each transaction conducted must be kept in a manner that will facilitate the reconstruction of such transactions.[98] A record should also be kept of all correspondence and analysis undertaken in relation to each transaction. A regulated business should ensure that evidence of transaction verification is documented and retained either with the transaction itself or in a manner that allows for ready or immediate recollection on request or as necessary, and readily available to the Designated Authority and Competent Authority.

ESTABLISHING SOW AND SOF

229. Pursuant to regulation 7A(5) of the POC-MLPR, a regulated business should obtain and verify both SOW and SOF for all business relationships and one-off transactions that have been determined to be high-risk.

230. SOW refers to the wealth or assets of the customer in general, whether they are the subject of a business relationship or not. The information to be obtained from an applicant for business should provide an indication as to the volume of wealth that the potential customer would reasonably be expected to have and the manner in which it was acquired.

231. SOW can be established by:

(a) obtaining information on the applicant's net worth—net worth can be obtained from the applicant's own representations;

(b) obtaining information on the source of the net worth—source normally includes: employment, investments, gifts and inheritance. Generally, there will be multiple sources accounting for the potential customer's net worth; and

(c) verifying information provided about the SOW—the SOW can be verified using reliable and independent sources that can be obtained (examples of which are in the table below); along with external confirmations and information provided by the applicant for business.

232. SOF refers to the origin of the particular funds or assets, which are the subject of the business relationship or one-off transaction between the regulated business and its customers, and the transactions being undertaken by these customers.

233. For transactions involving cash, verification of the SOF requires the conduct of additional due diligence measures to ensure that the funds were derived from a legitimate source.

234. Where funds originate from a third party, a regulated business should:

(a) Establish the relationship between its client and the person providing the funds;

(b) Establish the SOF;

---

[96] Regulation 7, POC-MLPR.

[97] The FID's reporting portal, goAML has established minimum standards for the acceptance of a report from a reporting entity. Therefore, any report submitted that does not have specified mandatory information will be automatically rejected by the system/portal.

[98] Regulation 14(4), POC-MLPR.

(c) Verify the SOF;

(d) Establish the purpose of the transaction; and

(e) Assess whether the transaction is in keeping with the documented financial profile of the customer.

235. SOF and SOW verification documents include (but are not limited to):

TABLE 5— SOF/SOW Verification documents

SOF/SOW	INFORMATION AND VERIFICATION DOCUMENTS
Employment Income	• Letter from employer • Annual salary • Pay slips (3 most recent) • Latest accounts or income tax declaration (if self-employed)
Savings/Deposits	• Bank statements • Passbook
Property Sale	• Details of the property sold (address, sale value, purchaser, date of sale) • Copy of signed sales agreement, Copy Certificate of Title
Sale of shares or other investment	• Copy of contract • Sale value of shares and name of dealer • Statement of account • Transaction receipt • Board resolution for sale of shares • Date of sale
Loan	• Copy of Loan agreement • Amount, date and purpose of loan • Name and address of lender • Details of any security/collateral • Statement of account
Company Sale	• Copy of the contract of sale • Name and address of the company • Companies Office search • Total sales price • Clients' share participation • Nature of business • Date of sale and receipt of funds • Open-source information (media etc.)
Company profits/dividends	• Copy of most recent audited financial statements • Copy of most recent in-house financial statements • Board of Directors' approval • Dividend distribution • Tax declaration form • Evidence of dividend payments
Inheritance	• Name of deceased • Date of death • Relationship to customer • Date received • Amount received • Attorney-at-law/Administrator/Executor details

TABLE 5— SOF/SOW Verification documents, *contd.*

SOF/SOW	INFORMATION AND VERIFICATION DOCUMENTS
Gift	• Date received • Amount received • Relationship to customer • Deed of Gift or Letter from donor explaining the reason for the gift and providing information on the source of the donor's wealth • Certified identification documents of donor
Maturity/Surrender of life policy	• Amount received Policy provider • Policy number/reference • Date of surrender • Statement of account
Other income sources	• Nature of income • Date received • Name of source • Letter from payer • Statement of account • Appropriate supporting documentation

Supplementary Requirement for Insurance Businesses

236. For insurance contracts, an insurance business is required to identify and verify the identity of the beneficiary. Verification can be done at the time of the pay out of the funds.[99]

237. Where the beneficiary is designated other than by name (for example, by reference to characteristics or a class) the insurance business shall obtain sufficient information to enable it to identify and verify the identity of the beneficiary at the time of pay out. After the beneficiary has been identified, the regulated business must then make a determination as to whether EDD measures are applicable. If so, such EDD measures are to be applied accordingly.

ENHANCED DUE DILIGENCE REQUIREMENTS

238. Pursuant to regulation 7A(1) of the POC-MLPR, each regulated business is required to establish a risk profile of all its business relationships and one-off transactions. Where a business relationship or one-off transaction has been determined by the regulated business to be high-risk, EDD measures should be applied. EDD is the application of additional CDD measures to mitigate the higher ML/TF risks.

239. The establishment of risk profiles involves *inter alia*—

(a) Conducting an assessment as discussed above in Section IV of the Guidelines. 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 national risk assessment;

(c) Ensuring the assessment is kept up-to-date (i.e. assessments being undertaken at least annually 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 regulated business to monitor whether its operations are consistent with the risk assessments and risk profiles that it has generated.

Enhanced Requirements

240. Heightened requirements are applicable where the risk of either doing business or establishing or maintaining certain relationships with certain customers or counterparties increases. Such circumstances of increased risk arise, for instance—

(a) by virtue of the positions held or functions undertaken by the customer or transacting counterparty; or

(b) in relation to customers or transacting counterparties in respect of which the regulated business will either have very limited or no 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.

[99] Regulation 13(1)(c)(iii)(D), POC-MLPR.

241. 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 supervisory AML/CFT/CPF 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—

(a) The financial activity is not subject to any regulation or supervision, nor 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/CPF laws and regime; and

(c) The existence of secrecy laws and other legislative or policy requirements adversely impact or hinder or prevent effective regulatory collaboration or cooperation from taking place between the FSC and the regulatory/supervisory authorities in that jurisdiction.

242. Under POC-MLPR and TP-RER, relationships or transactions that are identified as high-risk include—

(a) Persons holding specified state positions including politically exposed persons (PEPs) [see PEPs listing below];

(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*.

243. 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*.

244. Additional circumstances which, based on the foregoing, appear to increase the risks to a regulated 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) High net worth clients;

(f) Transferring clients;

(g) Transactions by emerging technology;

(h) Payable through accounts;

(i) Clients from countries with inadequate frameworks with respect to AML/CFT/CPF;

(j) Transactions undertaken for occasional customers; or

(k) Wire transfers and other electronic funds transfers.

245. Regulation 7A(4) of the POC-MLPR and Regulation 6A(4) of the TP-RER require that, where a business relationship or one-off transaction is determined to be high-risk, a business in the regulated sector shall carry out enhanced due diligence measures which includes the following—

(a) Obtain senior management approval to commence or continue the business relationship or one-off transaction;

(b) Verification of the source of funds or wealth held by the applicant for business and all other persons concerned in the business relationship or one-off transaction;

(c) A requirement that the payment in the first transaction be carried through an account with a financial institution in the name of the applicant for business; and

(d) Enhanced monitoring throughout the course of the business relationship or one-off transaction to include:

(i) a requirement for more frequent updating of customer information;

(ii) a requirement for more detailed information as to the nature of the business relationship;

(iii) a requirement for more detailed information about the applicant for business and other parties involved in the transaction;

(iv) an increase in the number and timing of controls applied to each relevant transaction; and

(v) the selection of patterns of actions that require more detailed examination.

Introduced Business[100]

246. In the case of a reliable introduction of a customer from an eligible regulated institution, preferably in the form of a written introduction, verification may not be needed. As a matter of course, the regulated business should immediately obtain and review the required identification data and other relevant documentation relating to customer identification as outlined above, from the introducing institution.

---

[100] Regulations 7 and 12, POC-MLPR; Regulations 5 and 12, TP-RER; FATF Recommendation 17.

247. In circumstances where business is being introduced, the ultimate responsibility is on the recipient regulated business to know the referred customer and his business and to establish the adequacy of the KYC/CDD details regarding this introduced business. Regulated businesses may rely on the identification procedures that the introducers have performed if the circumstances outlined in TP-RER, Regulation 12(1); and POC-MLPR, Regulation 12(l)(a) are in place. At a minimum, regulated businesses must—

(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/CPF laws and framework which govern the introducer;

(b) be satisfied that, based on the risk profile[101] the customer or transaction is not high risk;

(c) 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;

(d) 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, but within fourteen (14) days, after the introduction; and

(e) a regulated business' compliance with this requirement will be assessed by the Supervisor based on the availability of the CDD and KYC information for review by the Supervisory Authority.

248. In the event that any of the above conditions is not met, the institution should undertake and complete its own verification of the subjects arising out of the application for business either by—

(a) carrying out the verification itself; or

(b) relying on the verification of others in accordance with the Guidelines.

249. Upon the termination of the services of the introducer, responsibility for the integrity of records rests with the regulated business as product provider.

250. Where a transaction involves an institution and an intermediary, each needs separately to consider its own position to ensure that its own obligations regarding verification and recordkeeping are duly discharged.

Trust Accounts

251. Where an account is being opened by a trustee, settlor, or grantor, pursuant to trust arrangements, the identity of all parties, beneficiaries and ultimate beneficiaries or the person who exercises effective control of the trust must be ascertained and recorded in keeping with the POC-MLPR and the TP-RER[102]. This would include 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 terms of the trust arrangement for the trust or settlement.

Accounts Opened By Professional Intermediaries[103]

252. Professional intermediaries generally include collective investment schemes and pension fund managers/administrator, lawyers, securities dealers, stockbrokers and insurance agents and brokers. A regulated business may rely on the professional intermediary's customer identification due diligence process but only where there is compliance with the POC-MLPR and TP-RER.

253. Regulated businesses 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-MLPR that only permit reliance on third parties where the third party is itself subject to an AML/CFT/CPF regulatory framework.

254. It is important to note that while Attorneys fall within the FATF category of DNFBPs/gatekeepers in relation to the AML/CFT framework, Attorneys in Jamaica are exempt from the suspicious transaction reporting obligations of POCA and TPA[104]. Accordingly, when conducting business with an Attorney acting as a professional intermediary in respect of any one or more of the activities reflected in the DNFI designation orders under POCA and TPA, a regulated business should not rely on the due diligence processes of this person. Accordingly, at a minimum, a regulated business is required to ensure that—

(a) Records reflect the particulars of the accountholder (the Attorney), signing authorities and persons with the authorization to operate the account;

(b) It accesses and retains the relevant KYC information on account beneficiaries from the Attorney, as well as the transaction type and payment arrangement;

(c) It conducts its own verification of source of funds and wealth;

(d) Beneficiaries are not persons on UN list of terrorists or any other relevant watch list; and

(e) That the operation of accounts is consistent with the advised transaction(s) or payment arrangement.

255. If the intermediary is a locally regulated business and the account is in the name of the institution but on behalf of an underlying customer, then that customer should be subject to verification. If the account is to be in the underlying customer's name but the intermediary has the authority to conduct transactions, then the intermediary should be treated as a verification subject.

---

[101] Regulation 7A, POC-MLPR; Regulation 6A, TP-RER.
[102] Regulations 11, 12 and 13, POC-MLPR; Regulations 11, 12 and 13, TP-RER.
[103] Regulations 11, 12 and 13, POC-MLPR; Regulations 11,12 and 13, TP-RER; FATF Recommendation 17.
[104] JAMBAR v GLC and AG [2020]JMCA Civ 37. The Court of Appeal has ruled that Attorneys-at-Law are exempt from the following sections of POCA: 91A(2), (save and except for 91A(2)(b)); 94(2) and 95 and certain provisions of the POC-MLPR.

High Net Worth Clients

256. Institutions that offer specialized services for high-net-worth persons[105] must ensure that enhanced due diligence policies and procedures are developed and clearly documented. Senior management with ultimate responsibility for such services should ensure that the personal circumstances, income sources and wealth of high-net-worth clients are known and verified as far as possible and should also be alert to sources of credible third-party information. Whilst efforts must be made to protect the confidentiality of these customers and their businesses, these accounts must be available for review by the Supervisory Authority, the institution's internal compliance officers and internal and/or external auditors. The approvals for these business relationships must be obtained from at least one senior officer, other than the relationship manager.

PEPs

257. PEPs are individuals who are or were entrusted with prominent public functions and have been deemed high risk. This category of persons includes the following persons and their relatives[106]and close associates[107]—

(a) A head of state or of government;

(b) A member of any house of parliament;

(c) A minister of government;

(d) A member of the judiciary;

(e) A military official above the rank of Captain;

(f) A member of the police force of or above the rank of Assistant Commissioner;

(g) 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;

(h) A Director or Chief Executive of any company in which the Government owns a controlling interest;

(i) An Official of any political party; or

(j) An individual who holds, or has held, a senior management position in an international organization.

258. Given the risk assessment profile requirements under the AML/CFT regulations, as well as the risk based approach contemplated by the FATF Recommendations, a regulated business 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 POC-MLPR and at regulation 6A(6) of the TP -RER. These persons include former PEPs or middle ranking or junior officials acting in the name of, or on behalf of or for a PEP. This action may arise from a regulated business' own risk assessment where 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 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) and which gives the individual the authority to make decisions or issue directives regarding the use of public property; and

  (ii) the function undertaken by the individual exists in relation to an environment in which the risk of corruption or abuse is considered to be very high (e.g. minimum 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); or

  (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 the individual meets the criteria of a close associate of a person at (a) or (b).

259. Persons who qualify for classification as a PEP can remain subject to an assessment of high risk even after the termination of his/her appointment, as the basis for such treatment should be on risk and not on prescribed time limits.[108]

260. A regulated business should not establish business relationships with PEPs if the institution knows or has reason to suspect that the funds were derived from corruption or misuse of public assets.

261. To mitigate the significant legal and reputational risk that regulated businesses may 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 reasonably allow the regulated business 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 regulated business should also access publicly available information to assist in the determination and confirmation of whether or not an individual is a PEP;

---

[105] Includes Accredited Investors as defined by the Securities Act.

[106] Relatives, in relation to the person concerned, mean spouse, child (including stepchild or adopted child), the spouse of his child, his parents, his brother or sister. See Regulation 7A (7), POC-MLPR.

[107] Close associate means an individual who is a business partner, or associated in any other form, in a common commercial enterprise with the person concerned. See Regulation 7A (7), POC-MLPR.

[108] FATF Guidance on Politically Exposed Persons (R12 and 22), June 2013.

(b) 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;

(c) 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 serve to either substantially mitigate the risks associated with being a PEP, or exacerbate those risks;

(d) 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.

262. Following the commencement of business relationships, there shall be—

(a) Regular reviews of customer identification records to ensure they are kept current; and[109]

(b) On-going monitoring of PEP accounts.

263. The abovementioned procedures shall also be followed for the ultimate beneficial owners of bodies corporate or legal arrangements which are confirmed to be PEPs, as well as for the existing[110] client base to ensure that all current PEPs have been so identified and remain subject to enhanced CDD processes.[111]

Emerging Technology[112]

264. Regulated businesses should proactively assess the various risks posed by emerging technologies in the use of new payment products and services, and design customer identification procedures with due regard to such risks. New payment products and services (NPPS) are described in the related FATF Guidance[113] as new and innovative payment products and services that offer an alternative to traditional financial services. INPPS also involve new ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems and/or products that do not rely on traditional systems to transfer value between persons.

265. Risks posed by NPPS should be identified, assessed and understood before regulated businesses seek to establish their CDD processes and procedures and prior to the launch of such services 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.[114]

Virtual Currencies ("VC")

266. A VC[115] is a digital representation of value available only in electronic form. It is rarely issued or guaranteed by any jurisdiction and is intended only for online use. VCs are normally issued by private parties and are distinct from digital representations of central bank-issued currency, also known as central bank digital currency. The FATF Guidance indicates that VC's global reach increases its potential AML/CFT risks.

267. VCs can be traded on the internet, 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.[116] Therefore, VC payment products and services (VCPPS) present ML/TF risks and other crime risks that must be identified and mitigated.

Specified Territories and Countries with Inadequate AML/CFT Frameworks[117]

268. Regulated businesses must exercise added care when dealing with clients residing in countries with weak or non-existent laws and regulations to detect and prevent ML/TF/PF. A regulated business' assessment and risk-based approach regarding the countries identified as posing AML/CFT/CPF risks should be clearly outlined in its policy manual and updated, whenever necessary. In identifying these jurisdictions, regulated businesses may refer to the FATF's list of countries that have been identified as having strategic deficiencies in their AML/CFT/CPF frameworks.

269. The commencement of business relationships with clients residing in countries with inadequate frameworks must be subject to the KYC processes discussed above in this section and must have the prior approval of senior management. FATF has indicated that countries can employ possible countermeasures to mitigate the risks involved, including the following[118]:

(a) Requiring regulated businesses to apply specific elements of EDD;

(b) Introducing enhanced 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/CPF systems;

---

[109] Regulation 7(1)(c), POC-MLPR.
[110] Regulation 19, POC-MLPR.
[111] FATF Guidance on Politically Exposed Persons (R12 and 22), June 2013.
[112] FATF Recommendation 15.
[113] FATF Guidance on Prepaid Cards, Mobile Payments and Internet-Based Payment Services, June 2013.
[114] FATF Guidance for a risk-based approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services, June 2013—paragraphs 61 and 62.
[115] FATF Guidance for a Risk Based Approach—Virtual Currencies, 2015.
[116] Ibid.
[117] See FATF Recommendation 21.
[118] FATF (Revised) Recommendations—Interpretive Note to R19.

(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/CPF systems;

(e) Limiting business relationships or financial transactions with the identified country or persons in that country;

(f) Prohibiting regulated businesses from relying on third parties located in the country concerned to conduct elements of the CDD process;

(g) Requiring increased supervisory examination and/or external audit requirements for branches and subsidiaries of regulated businesses based in the country concerned;

(h) Requiring increased external audit requirements for financial groups with respect to any of their branches and subsidiaries located in the country concerned.

270. Pursuant to section 94A of POCA, the FSC has designated the following jurisdictions as specified territories as per notice in the *Gazette* published on November 23, 2021—

(a) Democratic People's Republic of Korea ("DPRK"); and

(b) Iran.

271. Regulated businesses are therefore required to treat all business relationships and transactions with customers resident or domiciled, and in the case of a corporate body, incorporated in a specified territory as follows—

(a) Apply EDD procedures;

(b) Ensure that the background and purpose of all such relationships and transactions ("R and T Analysis") are examined;

(c) Ensure that the findings of the EDD procedures and the R and T Analysis are committed to writing;

(d) Ensure that the findings are made available upon request to the FSC and the FID as the case may require; and

(e) Limit those business relationships or one-off transactions.

272. These actions must be taken in conjunction with the enhanced ML/TF countermeasures outlined in regulation 7B of the POC-MLPR and regulation 6B of the TP-RER. Those countermeasures are any directions from the FSC to regulated businesses which—

(a) Institute transaction or relationship limits;

(b) Require more frequent intervals for the provision of certain reports;

(c) Require the conduct of additional audit requirements; and

(d) Deny any exemption of identification procedures.

Transactions Undertaken for Occasional Customers[119]

273. An occasional customer (e.g., 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'[120]. 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[121]. Where a regulated business 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 requirements set out above, and all documents, reference numbers and other relevant details relating to the transaction should be recorded and retained by the regulated business for a minimum period of seven (7) years[122].

Anonymous Accounts/Accounts in Fictitious Names/Numbered Accounts

274. A regulated business must not conduct any transaction by means of an anonymous account, an account held in a fictitious name[123] or an account identified only by a number[124]. An anonymous account includes an account for which there is no name, by which the account holder can be identified. A numbered account refers to an account that is identifiable solely by reference to the number or series of numbers assigned to that account.

275. 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.

Other Activities/Transactions that may Trigger the Application of EDD Measures

276. EDD measures may be triggered by the following activities/transactions—

(a) Requests from foreign persons to establish accounts with a regulated business that is unaccustomed to maintaining accounts for overseas customers and which has not sought out such business;

(b) Requests for secrecy with transaction e.g., booking transaction in name of another person or entity whose beneficial owner is not disclosed or readily apparent;

---

[119] Regulation 6, POC-MLPR; Regulation 4, TP-RER.
[120] Regulation 2, POC-MLPR; Regulation 2, TP-RER.
[121] Regulation 6(l)(a), POC-MLPR.
[122] Regulation 14(5), POC-MLPR.
[123] FATF Recommendations 9 and 10; Section IV of The Guidelines.
[124] Regulation 16, POC-MLPR; Regulation 16, TP-RER.

(c) Routing of transactions into or through a secrecy jurisdiction;

(d) Deposits or withdrawals of multiple monetary instruments just below reporting threshold on or around same day;

(e) Patterns, where, after deposit or wire transfer is received, funds are soon thereafter transferred to another institution (particularly offshore or secrecy jurisdiction);

(f) Frequent minimal balance or zeroing out of an account for purposes other than maximizing the value of the funds held in the account e.g., placing the funds in an overnight investment and having the funds then return to the account;

(g) Enquiry by or on behalf of a PEP regarding exceptions to reporting requirements;

(h) The transaction is complex, unusually large or with an unusual pattern and does not make any economic sense; or

(i) The customer or parties involved in the transaction are from a specified territory.

SIMPLIFIED DUE DILIGENCE (SDD) PROCEDURES

277. Pursuant to regulation 7A (5A) and (5B), SDD procedures may be applied when a regulated business has made a determination that both the applicant for business and the product that is being accessed by the applicant are low risk. A regulated business is still expected to identify the applicant for business and take reasonable measures in verifying the identity of the applicant, despite the utilization of SDD procedures.

Conditions for Applying SDD

278. In determining whether SDD is applicable, the regulated business should:

(a) Conduct a proper evaluation of the risk to justify the adoption of the SDD procedures;

(b) Identify and document the risks of ML and TF;

(c) Implement appropriate controls and systems to reduce or mitigate those risks;

(d) On an ongoing basis, review both the identified risks and the systems/controls that have been implemented to mitigate those risks; and

(e) Review the product features of the business, such as:

(i) Threshold limits for the value of transactions;

(ii) Whether or not cross-border transactions are permitted;

(iii) Whether there is prohibition of the anonymous use of the product; and

(iv) Limits on delivery channels such as limited to face-to-face.

279. Where there is any change to the risk level of the business relationship, the regulated business should immediately apply the appropriate due diligence measures to the business relationship; that is, CDD for moderate risk customers and EDD for high-risk customers.

SDD Procedures

280. Pursuant to regulation 7 A (5C) of the POC-MLPR, SDD procedures may include the following:

(a) Requiring only one form of identification. This identification should preferably be government issued, but regulated businesses may accept any form of identification as recommended by the FSC;

(b) Accepting identification verification from third parties who are under equivalent obligations with respect to customer identification and transaction verification procedures;

(c) Collecting only basic identification information such as names, addresses, and dates of birth;

(d) Reliance on publicly available documents or such other documents as the FSC may specify; and/or

(e) Such other procedures as the FSC may specify.

SECTION V (A)—VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

281. The FATF in its June 2019 Bulletin—Revision to Recommendation 15 requires that virtual asset service providers (VASPs)[125] be regulated for AML/CFT purposes. Countries are therefore required to apply the relevant measures under the FATF Recommendations to virtual assets (VAs) and VASPs.

282. VASPs operating in Jamaica will therefore be required to be licensed or registered and will be subject to adequate regulation and supervision or monitoring for AML/CFT purposes. VASPs are required to understand the nature and level of their ML/TF risks and to implement preventative measures commensurate with those risks.

283. A VA is defined as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes. The FATF definition includes both virtual-to-virtual and virtual-to-fiat transactions or financial activities or operations. VAs do not include digital representations of fiat currencies, securities or any other financial assets that are already covered under the AML/CFT regulatory framework. A VASP is any natural or legal person which as a business conducts any of the following activities for or on behalf of another person:

(a) Exchange between virtual assets and fiat currencies;

(b) Exchange between one or more forms of virtual assets;

---

[125] FATF updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, October, 2021.

(c) Transfer[126] of virtual assets;

(d) Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and

(e) Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

284. VASPs include VA exchanges and transfer services; some VA wallet providers, such as those that host wallets or maintain custody or control over another person's VA's wallet(s), and/or private key(s); providers of financial services relating to issuance, offer, or sale of a VA (such as in an Initial Coin Offering); and other possible business models.

285. Some of the elements to be considered when identifying, assessing and determining how best to mitigate the risks associated with covered VA activities and the provision of VA products and services are:

(a) The potentially higher risks associated both with VAs that move value into and out of fiat currency and the traditional financial system and with virtual-to-virtual transactions;

(b) The risks associated with centralised and decentralised VASP business models;

(c) The specific types of VAs that the VASP offers or plans to offer and any unique features of each VA, such as Anonymity-Enhanced Crypto-currency, embedded mixers or tumblers, or other products and services that may present higher risks by potentially obfuscating the transactions or undermining a VASP's ability to know its customers and to implement effective CDD and other AML/CFT measures;

(d) The specific business model of the VASP and whether that business model introduces or exacerbates specific risks;

(e) Whether the VASP operates entirely online (e.g., platform-based exchanges) or in person (e.g. trading platforms that facilitates peer-to-peer exchanges or kiosk-based exchanges);

(f) Exposure to Internet Protocol (IP) anonymizers such as The Onion Router (TOR) or Invisible Internet Project (I2P), which may further obfuscate transactions or activities and inhibit a VASP's ability to know its customers and to implement effective AML/CFT measures;

(g) The potential ML/TF risks associated with VASP connections and links to several jurisdictions;

(h) The nature and scope of the VA account, product or service (e.g., small value savings and storage accounts that primarily enable financially excluded customers to store limited value);

(i) The nature and scope of the VA payment channel or system (e.g., open-versus closed-looped systems intended to facilitate micro-payments or government-to-person/person-to-government payments); as well as

(j) Any parameters or measures in place that may potentially lower the provider's (whether a VASP or other obliged entity that engages in VA activities or provides VA products and services) exposure to risk.

SECTION V (B)—SPECIAL GUIDANCE REGARDING TREATMENT OF LISTED ENTITIES

286. Regulated businesses are required to determine on a continuing basis whether they are in possession of property for persons on the U.N. lists of terrorists or persons linked with terrorists[127]. Regulated businesses 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.

287. Regulated businesses should note that a person can be designated as a 'listed entity', by order of the Supreme Court in accordance with section 14 of the TPA on the application of the DPP. This designation and the application of targeted financial sanctions should be effected within 24 hours of the UNSC notification.

288. For the effective implementation of this requirement, the Ministry of Foreign Affairs and Foreign Trade coordinates closely with the DPP's office, which in turn immediately sends the Formal Order to the various competent authorities and the FID. Each competent authority then immediately informs its licensees/registrants of the Formal Order. Thereafter, each regulated business is required without delay to screen its customer database against the names listed on this Formal Order. Each competent authority, the designated authority and the Ministry responsible for foreign affairs should publish the Order within 24 hours on their websites.

289. A regulated business is required to report at least once in every four months, or on the request of the Designated Authority, whether or not it is in possession or control of property of a listed entity. In making this report, the regulated business is to comply with any directions given by the Designated Authority. This report is to be made *via* the FID's goAML reporting portal.

290. In meeting this obligation of determining whether it has control or possession of property of a listed entity, a regulated business is required to screen its databases against the UNSC consolidated listing of entities[128]. Screening should be done at the on-boarding stage, periodically (recommended timeframe is every two weeks, but not less than once monthly) and immediately on the notification of new or amended listings (by way of Formal Orders). Large[129] regulated businesses must employ automated systems for ongoing screening whilst medium and small businesses may employ either automated or semi-automated systems.

291. Regulated businesses may find that they are in possession of property for, or in relation to, the following:—

(a) Persons affiliated/connected 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.);

---

[126] Transfer means to conduct a transaction that moves a VA from a VA address or account to another.
[127] Section 15, TPA.
[128] This can be accessed in an electronic format on the UN website.
[129] Defined as businesses with more than 50 employees.

(b) Persons for which the names are very similar to those appearing on the list of listed entities and there is sufficient information to suggest that it is the same person or in the case of incorporated/unincorporated entities, the names are sufficiently similar to consider that it is a related entity to the listed entity;

(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, 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.[130]

292. FATF Recommendation 6 requires each country to implement a targeted financial sanctions framework to comply with the UNSC resolutions relating to the prevention and suppression of terrorism and terrorism financing. These resolutions require countries to freeze, without delay, the funds or other assets of, and to ensure that no funds or other assets are made available, directly or indirectly, to or for the benefit of, any person or entity designated as a listed entity.

293. In this regard, Section 14 (4A) of the TPA provides that any Order granted under section 14(1) includes a prohibition on property owned or controlled by or on behalf of a listed entity. A regulated business is therefore required to freeze any accounts, funds or assets for a listed entity that it has in its possession.

294. A regulated business should also report immediately to the FID of any action that it has taken with regards to any asset or property of a listed person.

SECTION V (C)—SPECIAL GUIDANCE—COUNTER— FINANCING OF PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

295. Regulated businesses must ensure due diligence programmes, policies, procedures and controls established pursuant to AML/CFT obligations[131] also incorporate measures to allow for the identification of proscribed entities, persons and jurisdictions and the implementation of measures to prevent proliferation financing.

296. The UNSC Resolutions Implementation (Asset Freeze—Democratic People's Republic of Korea) Regulations, 2013[132] ("DPRK Regulations") were issued pursuant to section 3 of the UNSCRIA and these Regulations outline Jamaica's mandates in relation to the directives of the UNSC 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.

297. 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:

(i) an entity designated in Annex I or Annex II to UNSC Resolution 2087 (2013); or

(ii) an entity designated by the UN Sanctions Committee or by the UNSC for the purposes of paragraph 5(a) of UN Resolution 2087 (2013) as a person in respect of which countries must freeze funds immediately, or other financial assets and economic resources which are in their territories, owned or 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 of the DPRK Regulations. (Regulations 5(1) and 6(1)).

298. Since 2013, the UNSC has issued several other Resolutions with respect to DPRK. There are also similar resolutions issued by the UNSC with respect to Iran.

299. A comprehensive listing of all UNSC designated persons can be accessed at UNSC's website at www.un.org/sc. Alternately, persons may access this information *via* a link on the FSC's website at www.fsciamaica.org.

300. Section 8A of UNSCRIA prevents any person in Jamaica or any Jamaican outside of Jamaica, in relation to a person or entity that is proscribed by section 3(2) of UNSCRIA or by an order made under section 3A of UNSCRIA from knowingly—

(a) Dealing directly or indirectly with any assets that are controlled by or on behalf of, or at the direction of, the person or entity that is proscribed, including funds derived or generated from assets owned or controlled directly or indirectly by that person or entity;

(b) Entering into or facilitating, directly or indirectly, any transaction in respect of assets referred to in paragraph (a);

(c) Providing any financial or other related services in respect of any assets referred to in paragraph (a) to, for the benefit of, or at the direction of, the person or entity; or

(d) Making any property or any financial or related services available, directly or indirectly, for the benefit of the person or entity, or converting any such property or taking steps to convert or disguise that the property is owned or controlled by or on behalf of the person or entity.

---

[130] Section 94(4), POCA.
[131] Regulation 5, POC-MLPR; Section 18, TPA.
[132] Schedule to the UNSCRIA

301. Once such assets have been identified, any dealings that occur in relation to such assets should be limited to the sole purpose of preserving the value of such assets. Regulation 5(4) 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.

302. Regulated businesses 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.

303. Under section 3(1) of UNSCRIA, the Minister may, subject to affirmative resolution, make regulations to give effect to decisions of the Security Council under Chapter VII of the Charter, within thirty (30) days after the date of adoption of such resolutions and which are required to be carried out by Jamaica under Article 20.

304. Section 3A of the UNSCRIA permits the Director of Public Prosecutions ("DPP") to make an application to a Judge of the Supreme Court for an order to declare any person proscribed by a decision of the Security Council to be so declared. This section facilitates giving a more timely effect to the Security Council Resolutions and the Order will remain in force until the passage of regulations under section 3(1).

305. Upon any such application by the DPP, the Judge may, by order, declare a person or entity to be a proscribed person or entity, as the case may require. This order must be published on the websites of the Ministry of Foreign Affairs and Foreign Trade and the Designated Authority within twenty-four (24) hours after the order has been made. There is also a requirement to have the order published in a daily national newspaper.

306. As required under section 14A of UNSCRIA, the FSC shall notify, in the prescribed manner, all its regulated entities of all designations and de-listing of proscribed persons and entities. The FSC will therefore publish this order on its website and send electronic correspondence to licensees/registrants advising of new or amended listings.

307. Regulated businesses are required to determine on a continuing basis whether they are in possession or control of assets owned or controlled by or on behalf of a person or entity proscribed by Regulation under section 3(2)(a).

308. Each regulated business is to report to the Designated Authority *via* its goAML portal, at least once in every four months, or in response to a request from the Designated Authority, whether or not it is in control of any proscribed asset. In making this report, a regulated business shall comply with any directions as may be given by the Designated Authority.

309. Regulated businesses should screen names and addresses against the consolidated list of designated persons and entities (including entities owned or controlled by them) published by the UNSC in the following circumstances:

(a) During the onboarding process;

(b) At regular intervals (preferably every two weeks but no less than once per month);

(c) Without delay on the receipt from the designated or competent authority (or through appropriate software systems) of new or amended listings.

310. Regulated businesses are also required to implement effective systems for the identification and detection of the persons, entities and transactions related to proliferation financing.

311. In the event that a regulated business identifies a designated/proscribed person as a customer, then TFS are to be imposed immediately by the regulated entity. The regulated entity cannot have any dealings with the assets of the designated person (account, property, motor vehicles, funds etc.) as these are now "freezable assets", unless the transaction is for the sole purpose of preserving the value of such assets. A report on this designated person must be immediately submitted immediately to the designated authority.

312. Where in relation to any jurisdiction identified by the UNSC, on which TFS should be imposed, and freezable assets or 'dealings' have been identified (whether in the form of accounts established, funds held, transactions facilitated or otherwise), and in the absence of implementing regulations, a regulated business may, where it is determined that this can be done within a legal framework, consider taking the following steps:

(a) confine any dealings in relation to such assets to the sole purpose of preserving the value of such assets;

(b) 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 UNSC Act; and

(c) report the holding or dealing of the freezable asset to the Designated Authority.

SECTION V (D) —ADDITIONAL GUIDANCE— HOLDING COMPANIES

313. With the 2013 amendments to the POCA, the Fourth Schedule thereto extended the category of 'regulated business', to include holding companies[133] 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 holding company or such other person bearing this responsibility is fully subject to the statutory AML obligations under the POCA and its attendant regulations.

314. The group policies and programmes should permit the sharing of information between companies within the group for the purposes of customer identification, transaction verification and risk management.

315. The policies should ensure the safeguarding of confidentiality of any information shared and govern the use of the information disclosed within the group.

316. A holding company is also subject to the mandates in relation to local and overseas branches and subsidiaries.

---

[133] These include financial holding companies under the BSA and prescribed holding companies under pending amendments to the FSC Act.

SECTION V (E) - ADDITIONAL GUIDANCE—BRANCHES AND SUBSIDIARIES

Branches and Subsidiaries

317. Regulated businesses are required to advise their branches/subsidiaries (resident in Jamaica or overseas)[134] of the provisions of the Jamaican AML/CFT/CPF laws together with the provisions of any applicable Guidelines insofar as the dealings of such subsidiaries or branches are affected. Overseas branches are not considered to be legally distinct from their local head office and are therefore subject to Jamaican laws.

318. Each regulated business is therefore required to assess the AML/CFT /CPF 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. Where the AML/CFT requirements in that jurisdiction fall short of the Jamaican requirements[135] the regulated business should ensure that appropriate additional measures to manage the ML/TF risks are developed, documented, implemented and communicated to the FSC.

319. Overseas-based subsidiaries and foreign branches of local regulated businesses must inform their local parent companies and local head offices if they are not in a position to observe AML/CFT/CPF 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 the FSC,[136] and ensure that appropriate additional measures to manage the ML/TF risks are developed, documented, implemented and communicated to the FSC. The FSC will then make a determination on the adequacy of the measures applied and any other required course of action that may also include closure of the relevant overseas subsidiary or branch.

320. Regulated businesses, that have local subsidiaries which are themselves subject to AML/CFT/CPF and other guidance from authorities other than the FSC (whether regulatory or otherwise) shall assess the AML/CFT/CPF guidance against which their subsidiaries operate and shall ensure that those subsidiaries apply the higher required standard.[137]

321. A regulated business shall ensure that its local subsidiaries engaged in financial services implement and conform to obligations under the POCA, the TPA, the UNSCRIA and attendant regulations, as well as the Guidelines.

322. 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. In addition, appropriate systems are required to combine cash transactions conducted at different branches in the same day to identify and prevent structuring.

Non-Financial/Non-Regulated Subsidiaries

323. Licensees/registrants should be in a position to prove to the FSC that the operations and activities of their non-financial and/or non-regulated subsidiaries do not pose a financial drain or a ML/TF risk to the regulated business. The level 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 company.

SECTION VI—THE NOMINATED OFFICER REGIME

The Appointment of a Nominated Officer

324. A regulated business must designate an employee of the institution who performs management functions as its Nominated Officer[138]. This Officer is responsible for ensuring the effective implementation of the established policies, programmes, procedures and controls to prevent and detect ML/TF activities in accordance with the relevant statutes, the Guidelines and the licensee's own policies and procedures.

325. The Nominated Officer position requires:

(a) Seniority in post to allow for reporting directly to the Board, or through a sub-Committee of the Board, on the institution's AML/CFT/CPF compliance;

(b) Extensive knowledge of the AML/CFT/CPF 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) The ability and capacity to undertake the responsibility for ongoing monitoring of the fulfilment of AML/CFT/CPF duties by the institution; and

(d) Independence[139] of the business lines of the institution to allow for an objective assessment, monitoring and enforcement of the compliance of the institution's operations and decision-making with its AML/CFT/CPF obligations under the country's framework and with the institution's own AML/CFT/CPF policies and procedures.

REPORTING OBLIGATIONS OF THE NOMINATED OFFICER

Reports to the Designated Authority[140]

326. The Nominated Officer is responsible for reporting to the Designated Authority,[141] all such activities and transactions as required by the relevant statutes and the Guidelines and should be in a position to provide advice and guidance to the staff. 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/CPF laws and should consult with the Designated Authority accordingly.

---

[134] Regulation 18, POC-MLPR; Regulation 18, TP-RER.
[135] Regulation 18, POC-MLPR; FATF Recommendation 18.
[136] Regulation 18(2), POC-MLPR; Regulation 18(2), TP-RER.
[137] Regulation 18, POC-MLPR; Regulation 18, TP-RER; FATF Recommendation 2.
[138] Regulation 5(3), POC-MLPR; section 18(3), TPA
[139] This requirement is not applicable to small businesses, that is businesses with up to 20 employees.
[140] Section IX of The Guidelines for detailed guidance on reporting requirements.
[141] Section 95, POCA; Section 18(3), TPA.

327. In keeping with reporting obligations under section 94 of POCA and internal reporting procedures under Reg. 15 of the POC-MLPR, the Nominated Officer is required to institute an internal reporting framework that facilitates a formal disclosure of reportable transactions by employees to the Nominated Officer within fifteen (15) days after having knowledge of the transaction or matter. The Nominated Officer should facilitate the use of the FID's goAML reporting portal for the making of these internal STRs by employees. The Nominated Officer is required to provide advice and guidance to the staff on the identification of suspicious transactions.

328. Any such reports received by the Nominated Officer under section 94 of POCA should be submitted to the Designated Authority within fifteen (15) days of their receipt unless the Nominated Officer knows or believes or has reason to know or believe that the transaction does not constitute or is related to money laundering. This report should be submitted to the FID *via* its goAML reporting portal.

329. Nominated Officers should be aware that suspicious transaction reports under section 16 of the TPA should be submitted by the institution as soon as is reasonably practicable, and in any event, within fifteen (15) days after the suspicion or reasonable cause for suspicion arises.

Reports to the Board of Directors

330. An institution's policy manual should require the preparation and submission of reports by the Nominated Officer to the Board of Directors (the Board), at least once per year or more frequently, as warranted by its risk profile. This is to ensure that 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 include, at a minimum:

(a) An annual overview and evaluation of the overall effectiveness of the institution's AML/CFT/CPF framework, the effectiveness of AML/CFT/CPF measures implemented under each of the various operational areas and product and service types, as well as AML/CFT/CPF training exercises completed, and initiatives pursued;

(b) The licensee's/registrant's compliance with relevant legislation and the Guidelines in relation to the institution's AML/CFT/CPF reporting obligations, as well as the entity's own policies and procedures;

(c) Particulars of the risk assessment and risk management activities (see Section IV) including:—

(i) Updates on the regulated business' overall relationship with the Designated Authority and general guidance received from that body; and

(ii) Advice on any proposed/impending legislative AML/CFT/CPF amendments, with an assessment of possible impact on the institution with appropriate proposals for the requisite operational changes required for continuing compliance.

BASIC DUTIES AND RESPONSIBILITIES OF THE NOMINATED OFFICER

331. The Nominated Officer should be responsible for the day-to-day monitoring of the financial institution's compliance with AML/CFT/CFP 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, the officer should have access to all operational areas and have the requisite seniority and authority to report independently to the board.

332. These duties must be independent of the internal audit function.

333. The duties and functions of the Nominated Officer should, at a minimum, include the following:

(a) Act as liaison between the institution and the FSC and other competent authorities with respect to compliance matters and investigations;

(b) Ensure that:

(i) risk assessments are carried out by the institution;

(ii) the appropriate risk profiles are established;

(iii) the relevant measures and mechanisms commensurate with the risks assessed are implemented; and

(iv) these assessments are kept up to date and relevant.

(c) Evaluate new products and services to determine the risk exposure of the institution;

(d) Assist business units in the implementation of the compliance programme, which includes informing and guiding the Board and the staff of regulatory changes;

(e) Ensure that there are adequate systems in place for monitoring transactions and for the identification and reporting of unusual and suspicious transactions;

(f) Receive and evaluate reports of unusual/suspicious transactions;

(g) Ensure the timely filing of Suspicious Transaction Reports (STRs), Suspicious Activity Reports (SARs); Threshold Transaction Reports (TTRs), Listed Entity Reports (LERs) and Proscribed Entity Reports to the Designated Authority;

(h) Request appropriate consent from the Designated Authority before conducting prohibited transactions;

(i) Coordinate with the institution's audit and legal departments on AML/CFT/CPF matters;

(j) Periodically provide reports to the senior management and the Board on the effectiveness of the AML/CFT/CPF framework;

(k) Prepare and update policies and procedures consistent with the requirements of the AML/CFT/CPF legislative framework which should be readily accessible to the institution's Board, management, staff, and other relevant personnel and parties who may be involved in the operations;

(l) Oversee administrative matters related to the Code of Conduct and Compliance with AML/CFT/CPF activities;

(m) Develop related training material and implement the required training regime;

(n) Maintain coordination among the nominated officer of each regulated entity within a group of companies;

(o) Carry out site visits to branches/units to observe implementation of internal controls procedures in compliance with established policy and procedure requirements;

(p) Utilize monitoring and audit systems to ensure compliance with all AML/CFT/CPF laws and requirements; and

(q) Ensure reviews of daily transactions in order to identify unusual/suspicious/potentially fraudulent activities, account excesses, etc.

CONFIDENTIALITY PROVISIONS

334. The Nominated Officer is to ensure adherence to the confidentiality provisions established under sections 97 and 104 of POCA, sections 17 and 20 of the TPA and section 5 of the UNSCRIA. Therefore, an institution should not disclose:

(a) That it has submitted a report to the Designated Authority;

(b) any information it has with respect to a forfeiture investigation, a civil recovery investigation, a money laundering investigation or a terrorism/proliferation investigation.

335. The institution should therefore have confidentiality procedures as follows:

(a) The requisite systems in place to ensure confidentiality of any court order served on it, except to the extent of complying with the order or acquiring legal advice from an Attorney-at-Law.

The existence of the court order must only be disclosed to other employees, if such disclosure is necessary to ensure that the relevant information is provided to fulfil the requirements of the order. The Nominated Officer should, in most cases, be responsible for ensuring that the order is complied with. He should be responsible for determining if other staff members "need to know" about the court order to assist with providing relevant information;

(b) Officers of the institution apprised of the order must not disclose its existence to other employees.

FIT AND PROPER REQUIREMENTS

336. A Nominated Officer has to be a fit and proper person, which means the Nominated Officer:

(a) has not been convicted of an offence involving dishonesty or of an offence listed in the Second Schedule of POCA;

(b) is not an undischarged bankrupt;

(c) is in compliance with any tax and other statutory requirements imposed by an authorized agency;

(d) satisfies such solvency and liquidity requirements as the FSC may specify; and

(e) is not associated with a company which, at the time of the association, is engaged in any breaches of any financial services legislation.

337. The Nominated Officer must also, in the opinion of the FSC, be a person:

(a) of sound probity, who is able to exercise competence, diligence and sound judgment in fulfilling his functions in relation to the licensee/registrant and whose relationship with the licensee/registrant will not threaten the interests of their clients;

(b) who possesses the knowledge, skills and experience which are necessary for the intended functions to be carried out by that person;

(c) who has not engaged in any business practice which appears to the FSC to be deceitful or oppressive or otherwise improper;

(d) who has not contravened any provision of any enactment designed for the protection of the public against financial loss due to dishonesty, incompetence or malpractice; and

(e) whose employment record does not give the FSC reasonable cause to believe that he carried out any act involving impropriety in the provision of any financial services or in the management of a company.

Fit and Proper Checks

338. The FSC will, on the appointment of a nominated officer and on an on-going basis, conduct an assessment of the fitness and propriety of the nominated officer. Institutions are required to advise the FSC of the appointment of the nominated officer in writing within fourteen (14) days and submit the following documents:

(a) Properly completed Fit and Proper Questionnaire for the relevant industry within which the nominated officer operates[142];

(b) Valid police record; and

(c) Current résumé.

339. Any change in the office of the nominated officer must be communicated to the FSC within fourteen (14) days of such a change being made. It is also advisable that institutions refrain from confirming a person as its nominated officer until it has received clearance from the FSC affirming the person's fit and proper status.

---

[142] The questionnaire may be accessed *via* the FSC's website.

SECTION VII—COMPLIANCE MONITORING

Internal Compliance Programme

340. An effective internal compliance programme is essential to an institution's endeavour to comply with its obligations under the law, prevent involvement in illicit activities and adhere to international standards.

341. Regulated businesses are required to have systems in place for an annual[143] independent audit to ensure that the statutory requirements and the programmes itemized in the Guidelines and adopted in policy manuals, are implemented. A Nominated Officer must have explicit and ultimate responsibility for the regulated business' internal compliance program, which at a minimum should involve:

(a) Establishment of an adequately resourced unit responsible for day-to-day monitoring of compliance;

(b) Establishment of a robust compliance plan that is approved by the Board of Directors of the institution and that provides for on-going independent review and testing of staff's compliance with AML/CFT/CPF 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 and Competent Authorities to ensure that the institution is carrying out its obligations under the law;

(f) Regular or periodic reviews of the AML/CFT/CPF program and the internal and external audit functions. The timing of these reviews should be informed by, among other things, the institution's risk profile.

342. The Nominated Officer must have access to all relevant information held by the regulated business needed to make a proper assessment as to whether a customer is engaged in ML[144].

POLICY AND PROCEDURAL MANUAL

343. Each regulated business shall establish clearly defined policies and operational procedures with respect to its obligations under the AML/CFT/CPF legislative framework which are informed by the institution's assessment of its risks as discussed in Section IV above. The AML/CFT/CFP policies and procedures should:

(a) be properly documented in the form of a manual which is readily available to staff (preferably in an electronic format) and staff must be informed of the available methods to access the manual; and

(b) be reviewed at least on an annual basis to ensure its continued compliance with legislative provisions and supervisory directions. All revisions are to be approved by the Board.

344. A regulated business' policies and procedures manual must include:

(a) measures and procedures which are commensurate to the risks that have been identified from the institution's assessment of its risks;

(b) procedures to ensure high standards of integrity for employees at all levels including senior and executive management levels;

(c) a system to evaluate the personal employment history and financial history of all employees at all levels including senior and executive management levels;

(d) programmes for the training of employees on a continuing basis, and at minimum on an annual basis;

(e) comprehensive CDD, EDD and SDD policies and procedures;

(f) controls, such as:

  (i) clear lines of authority and responsibility;

  (ii) segregation of duties;

  (iii) establishment of limits;

  (iv) monitoring of activities;

  (v) identification and monitoring of key risks; and

  (vi) new product/service approval process.

(g) The appointment of a Nominated Officer;

(h) procedures for analysis of clients' transactions to ascertain trends and to recognize indicators of unusual and/or suspicious activities;

(i) arrangements for annual independent (internal and/or external) audit reviews;

(j) procedures for documenting and maintaining records of transactions;[145]

(k) systems for identifying and reporting suspicious transactions;

---

[143] Small low risk businesses may institute longer periods for this independent assessment. The justification for the adoption of this relaxed policy must be in writing and available to the FSC on request. Small businesses are defined as businesses with up to 20 employees.

[144] Regulation 15, POC-MLPR.

[145] Regulation 14(4), POC-MLPR.

(l) procedures for maintaining a log reflecting large, complex and unusual transactions;

(m) systems for identifying and reporting threshold transactions;

(n) screening systems for identifying and reporting listed and proscribed entities;

(o) procedures for application of TFS;

(p) procedures for training of staff in the operation and implementation of procedures and controls relating to the combatting of ML/TF/PF, and their obligations under the law; and

(q) obligations for financial holding companies, and responsibilities in respect of branches and subsidiaries.

SECTION VIII—TRANSACTION MONITORING AND REPORTING

Transaction Monitoring

345. Regulated businesses are required to monitor their customers' transactions to ensure that they are in keeping with the financial and risk profiles of the customers. Transaction monitoring ("TM") is therefore a key control measure in the prevention of ML and TF. An effective TM system facilitates assessment of customers' transactions (inflows/outflows) over extended periods and therefore assists in the identification of any unusual or suspicious trends or patterns.

346. Large[146] regulated businesses are required to implement automated TM systems that are able to detect any unusual or irregular transactions or series of transactions. These systems should be configured with appropriate TM thresholds, scenarios and parameters that are aligned with specific risks and context. Some scenarios that should be factored into automated TM systems include:

(a) Large or complex transactions;

(b) Aggregated frequent and small (or below the threshold) transactions;

(c) Unusual patterns of cash deposits or withdrawals for which the accumulative value is large;

(d) Significant deviations from historical account activity;

(e) Transactions with nexus to higher risk countries;

(f) Pass-through payments;

(g) Circular flows involving opaque business structures;

(h) Tax evasion activities; and

(i) Transactions that have no apparent economic purpose.

347. Regulated businesses are required to pay particular attention to customers with multiple accounts (especially at different branches) and accounts that are related.

348. Small[147] businesses that rely on manual TM systems are required to conduct daily transactions reviews. It is recommended that these small businesses, institute, at minimum, semi-automated TM systems to assist in the identification of irregular or abnormal transactions. Reliance on a fully manual TM system may impede the identification of structured transactions or series of transactions that when aggregated may appear to be suspicious.

349. Where transactions exhibit reasonable grounds for suspicion of ML/TF, a regulated business is required to file a STR. Regulated businesses should also monitor the media and where applicable, file STRs on customers with adverse media reports.

REQUIRED DISCLOSURES—IDENTIFICATION AND REPORTING OF SUSPICIOUS TRANSACTONS

350. A suspicious transaction will often be inconsistent with a customer's known legitimate business, personal activities, the normal business for that type of account or with the nature of the transaction indicated. The critical elements in recognizing a suspicious or unusual transaction or series of transactions are—

(a) general knowledge of the nature of the industry/sector in which the customer operates;

(b) the nature and pattern of the customer's own business;

(c) a good understanding of the operating environment; and

(d) the financial processes that would be applicable to the various services and products offered.

351. A person within a regulated business is required to make a disclosure to either the Nominated Officer (or an authorised delegate) or to the Designated Authority, of information or other matters 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 ML, pursuant to section 94(3) of the POCA. Where a regulated business knows or believes, or has reasonable grounds for knowing or believing, that a customer or prospective customer is engaging in ML activities/transactions, 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) seek appropriate consent, through the Nominated Officer, from the Designated Authority to proceed with the transaction[148].

---

[146] Businesses with over 50 employees.
[147] Businesses with up to 20 employees.
[148] Sections 93(2), 99, 100(4) and (5), POCA.

352. The law requires that a suspicious transaction report under the POCA or the TPA is one that should be made either to the Nominated Officer or the Designated Authority[149]. In practice and for good order, reports within the regulated businesses may be made *via* the goAML reporting platform to the Nominated Officer who will thereafter be required to evaluate the disclosure and where merited, submit it to the Designated Authority.

353. Regulated businesses should establish internal reporting procedures that ensure that all matters identified for reporting under the TPA or POCA are brought to the attention of the Nominated Officer. Each report must then be reviewed to determine whether the suspicion is justified, and in the absence of information to negate the suspicion, the Nominated Officer should submit a report to the Designated Authority, within the stipulated statutory period. Under POCA, the employee who processed the transaction is required to disclose to the Nominated Officer as soon as is reasonably practicable and in any event within 15 days. The Nominated Officer then has a further 15 days within which to report it to the Designated Authority. Under the TPA, the reporting entity has fifteen (15) days in which to make the report to the Designated Authority. The specific steps that must be followed for the reporting of such transactions must be clearly outlined in the policy and procedural manual and communicated to all relevant personnel.

354. Under the TPA, each entity is required to report 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 in the commission of a terrorism offence or involve, or are for the benefit of, any listed entity or terrorist group.

355. In complying with the obligation to report suspicious transactions under the POCA and the TPA, a regulated business is also required to:—

(a) pay attention to (or identify and take notice of):

  (i) complex, unusual or large business transactions, or unusually large transactions carried out by the customer with the regulated business;

  (ii) unusual patterns of transactions;

  (iii) unusual employment of an intermediary in the course of some usual transaction or financial activity;

  (iv) unusual method of settlement; and

  (v) unusual or disadvantageous early redemption of an investment product.

(b) make a record of these transactions and the related findings[150];

(c) ensure that the findings and transactions are made available, on request, to its auditors, the Competent Authority and to the Designated Authority.

(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[151].

356. Severe implications such as prosecutorial and/or reputational risk can arise when a regulated business facilitates ML/TF/PF and fails to file STRs. The institution shall ensure that such accounts or transactions are subject to 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 a certain amount;

(f) refuse to undertake new business with the customer; and

(g) refuse to accept introduced business from that customer or in relation to that customer.

357. The application of appropriate countermeasures by a regulated business will be indicative of it 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 in question.

358. Regulated businesses should have adequate systems to ensure the timely, ongoing detection and reporting of suspicious and threshold transactions (where applicable), and holdings of property owned or controlled by a listed or proscribed entity.

359. Regulated businesses 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 outlines circumstances where the disclosure is made in carrying out a function the person has relating to the enforcement of any provision of the POCA or of any other enactment relating to criminal conduct or benefit from criminal conduct. A regulated business would however be expected to exercise discretion and judgment to ensure that in-house disclosures to internal auditors and disclosures to external auditors 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.

360. There are categories of activities that are suspicious by their very nature and should alert a regulated business to the possibility that a customer is seeking to use the institution as a conduit for ML/TF/PF activities. Examples of such suspicious conduct and activities are outlined in Appendix I. Regulated businesses should be aware of evolving typologies of ML/TF/PF.

---

[149] Section 94(3), POCA; Sections 18(3), 16(3) and (3A), TPA.
[150] Section 94(4)(a), POCA; Section 16(3)(b), TPA.
[151] Section 94(4)(b), POCA.

361. Regulated businesses should note that under the POCA any offence in Jamaica could constitute a predicate offence. 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.

362. Regulated businesses should provide all requisite statutory information to facilitate any investigation resulting from the report, and to ensure compliance with reporting obligations.

363. A regulated business is obliged to provide its reasons for determining that a particular transaction/activity is suspicious. The reasons for suspicion must:

(a) be sufficiently detailed, clear and precise;

(b) set out the rationale for suspicion;

(c) indicate the particular unusual nature of the transaction;

(d) provide contrasting historical data;

(e) provide information on related parties; and

(f) set out the chronology of events.

364. Regulated businesses should establish a reporting and feedback regime for required disclosures:

(a) On receipt of a report concerning a suspicious transaction/activity, the Nominated Officer should assess the details to determine whether in all the circumstances a report should be submitted to the Designated Authority.

(b) If the Nominated Officer decides that:

(i) the information substantiates a suspicion of ML/TF, then this information should be disclosed within the statutory timeframe;

(ii) there is uncertainty as to whether such information substantiates a suspicion, then it should nevertheless be reported; or

(iii) the information does not substantiate a suspicion, then the reasons for not submitting the report to the Designated Authority must be recorded.

(c) The regulated business' treatment of the matter subsequent to the disclosure being made must be in accordance with the statutory feedback regime termed "appropriate consent" which can be found under sections 91, 99 and 100 of the POCA.

365. In the case of a regulated business that is a part of a group of companies, the responsible person for the group shall establish programmes, policies, procedures and controls that facilitate the detection or prevention of ML within that group of companies. The group's programmes, policies, procedures shall:

(a) permit the disclosure of information among companies within the group, for the purposes of customer identification, transaction verification and risk management, other than information which is protected from disclosure;

(b) ensure the safeguarding of confidentiality and govern the use of the information disclosed within the group.

Appropriate Consent Regime

366. For regulated businesses, "appropriate consent" occurs in the following circumstances:

(a) when the Nominated Officer receives consent from the Designated Authority within seven business days of the Nominated Officer's disclosure and request for consent to undertake the prohibited transaction[152];

(b) after the Nominated Officer makes a disclosure to the Designated Authority, and that Officer has not received a response from the Designated Authority within seven business days[153];

(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 business days denying consent, but ten days have passed since the receipt of that notice[154].

367. The POCA provides for the granting 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 written notification[155].

368. If the institution is convinced that it must proceed with the transaction, relationship or arrangement, before making the relevant disclosure and securing the appropriate consent then the institution must:

(a) have a reasonable excuse for failing to make the disclosure before proceeding with the transaction;

(b) make the relevant disclosure on its own initiative; and

(c) make the said disclosure as soon as is reasonably practicable[156].

---

[152] Section 99(l)(a), POCA.
[153] Sections 91(2)(b)(i) and 99(1)(b), POCA.
[154] Sections 91(2)(b)(ii) and 99(l)(c), POCA.
[155] Section 99(4), POCA.
[156] Sections 93(2), 99(1) and (2), 100 (4) and (5), POCA.

369. Regulated businesses should also note the following:

(a) if the institution has a reasonable excuse for failing to make the disclosure before proceeding with the transaction, relationship or arrangement, then the institution must ensure that the relevant disclosure is made on its own initiative and as soon as is reasonably practical[157].

(b) further to (a) the institution must seek the necessary guidance, directive or consent from the Designated Authority before it continues to offer any service or facility to that customer against whom the suspicion of ML remains.

370. Regulated businesses must therefore satisfy themselves that the direction or consent obtained from the Designated Authority clearly permits or prohibits the doing or undertaking of any activity in relation to accounts, transactions, customers or property in respect of which authorized disclosures have been made.

371. The Appropriate Consent regime does not apply under the TPA. Therefore, where a regulated business is uncertain whether a transaction breaches either the provisions of POCA or the TPA, the regulated business should make the disclosure under POCA. Making the disclosure under the POCA allows for the utilisation of the appropriate consent regime, if necessary.

Unusual, Large and Complex Transactions

372. The requirement to "pay attention to" or "pay special attention to" certain transactions, as used in section 94(4)(b) of POCA and section 16(3) of the TPA respectively, includes:

(a) identifying and taking notice of the types of transactions described in these sections of the law;

(b) the examination of the background and purpose of these types of transactions;

(c) the formal recording of the institution's findings; and

(d) the retention of the institution's findings for a period not less than 7 years.

373. Regulated businesses must make the log of unusual transactions available to the FSC and the Designated Authority, upon request.

Protected Disclosures

374. Sections 100 and 137 of POCA treat with protected disclosures;

(a) Under section 100 (1), (2) and (3) a disclosure is protected if it satisfies the following conditions:

(i) The information or other matter disclosed came to the person making the disclosure in the course of that person's trade, profession, business or employment;

(ii) The information or other matter causes the person making the disclosure to know or believe, or to have reasonable grounds for knowing or believing that another person has engaged in ML; and

(iii) The disclosure is made to an authorized officer or Nominated Officer as soon as is reasonably practicable after the information or other matter, which gives rise to the knowledge or belief or reasonable grounds for such knowledge or belief, comes to the person making the disclosure.

(b) Under section 137 of POCA there is no civil or criminal proceedings for breach of confidentiality, 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 or the Competent Authority.

375. Section 16 (7) of the TPA has provisions for the protection of persons who provide or transmit information requested or submit reports to the Designated Authority.

Tipping Off Provisions

376. A regulated business is under strict obligations not to disclose to any person, the fact that it has made a required disclosure pursuant to section 94 or 95 or an Authorized Disclosure pursuant to section 100 of the POCA; or has 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.

---

[157] Section 100(4) and (5), POCA

377. The regulated business may reveal the existence of an authorized disclosure under the following circumstances:

TABLE 6—CIRCUMSTANCES OF DISCLOSURE

Section	POCA/TPA	The Circumstances of Disclosure
97(2)(a)	POCA	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.
97(2)(b);97(3)(a)	POCA TPA	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	The disclosure is made to the Competent Authority.
17(2)(a); 17(4)(a)	POCA	The disclosure is made to any person in connection with legal proceedings or contemplated legal proceedings.

Post-STR Requirements

378. Once an STR has been submitted on a customer, that customer should immediately be classified as high risk and EDD procedures must be applied to all subsequent transactions on that account. If the regulated business decides to retain the business relationship then it should apply the following additional enhanced measures to the account:

(a) Seek appropriate consent from the FID for any transaction that appears irregular, unusual or suspicious;

(b) Implement senior management approvals for transactions exceeding a defined threshold;

(c) Flag the account to ensure that all staff is aware that any transactions on this account require enhanced scrutiny; and

(d) Place limits on the number and types of transactions conducted on the account.

TABLE 7—Summary Listing of All Reports to be Submitted to the FID *via* the goAML Reporting Portal.

Legislative Reference	Type of Report	Frequency	Due Date	Comments
POCA S.94/95	Suspicious Transaction Report (STR)	Ongoing	15 days for conductor of transaction to the report to the Nominated Officer; and thereafter 15 days for the Nominated Officer to report to the FID.	An employee can of report directly to the FID, but it is recommended that for orderly submission of reports, report are made to the Nominated Officer. A STR is filed where the suspicion arises after the transaction has been concluded.
POC-MLPR Reg. 3	Threshold Transaction Report (TTR)	Monthly	15 days after the end of each month.	This report is to be made only by financial institutions and must be made whether or not there is a reportable cash transaction.
POCA S. 100(4)	Authorised Disclosure and Request for Consent	Ongoing	As soon as is practicable before conducting the transaction.	This report is applicable where the suspicion arises before the transaction is conducted. The Nominated Officer is required to seek appropriate consent from the FID before procedding with the transaction or decline the transaction.
TPA S. 16	Suspicious Transaction Report (STR)	Ongoing	As soon as is practicable but within 15 days.	Unlike POCA, under the TPA the institution has only 15 days file to the STR.
TPA S. 15	Listed Entity Report	Every 4 months	Within 1 month after the end of each 4-month period.	3 reports are to be made annually by: May 31, September 30 and January 31.
UNSCRIA S.5[158]	Proscribed Entity Report	Every 4 months	Within 1 month after the end of each 4-months period.	3 reports are to be made annually by: May 31, September 30 and January 31.

SECTION IX—RECORDKEEPING REQUIREMENTS

379. On the inception of a business relationship, a regulated business is required to maintain the following records:

(a) client information collected during the KYC/CDD process;

(b) each transaction;

(c) all correspondence with the customer;

(d) account files; and

(e) any analysis conducted in relation to each transaction and the business relationship.

380. Account files must be kept for each customer containing all pertinent information including: account numbers, types of accounts, full customer identification information, account opening documentation, business correspondence and a summary of the activities in respect of each account.

381. Transaction records must be maintained in such a form that allows for reconstruction of each transaction and for the provision of information to the Designated Authority or the Competent Authority within 7 days of such a request. At a minimum, transactions records maintained should include the date and details of a transaction, the amounts and currencies involved and information on the conductor (agent) of the transaction.

382. The relevant legislation has provisions that require the production of records and documents or the access to such records and documents by the Competent Authority, the Designated Authority or an authorized officer upon appropriate authority.

383. Retention of documents must be for seven (7) years in a form admissible under the Evidence Act. Where records relate to an on-going investigation or have been the subject of a court order, they should be retained beyond the statutory seven-year period until the Designated Authority has indicated that there is no longer a requirement for such records.

---

[158] There is no requirement to submit a STR under the UNSCRIA.

384. For electronic transactions, the Electronic Transactions Act has been in effect since April 2007 and treats with the:

(a) validity of electronic transactions (section 6);

(b) requirements to give information in writing (section 7);

(c) requirements for signature (section 8);

(d) requirements for attestation etc. of documents (section 9);

(e) requirements to produce a document for inspection or in original form (section 10);

(f) requirements for keeping information (section 11); and

(g) admissibility and evidential weight of information in electronic form (section 12).

SECTION X—BOARD RESPONSIBILITY AND EMPLOYEE INTEGRITY AND AWARENESS

Board Responsibility

385. The Board of Directors of a regulated business must have a clear understanding of the ML/TF risks faced by the institution. The Board must also be actively aware of the risk framework and processes affecting the institution, Where it is a part of a financial group, or a broader corporate structure consideration must also be given to broader risks posed to the institution.

386. Regard must also be had to risks from the national perspective which includes:

(a) performance of the economy;

(b) levels of crime and types of crimes to which financial services are most vulnerable;

(c) the country's external ratings in the areas of credit risk, transparency, and cooperation; and

(d) inclusion on watch lists, or sanction lists.

387. The Board of a regulated business must be satisfied that:—

(a) the institution's risk assessment is accurate and that measures to mitigate the risks identified are effective and reviewed on an ongoing basis.

(b) the Nominated Officer is appropriately qualified and has the requisite authority to effectively undertake the responsibilities of that function.

(c) the reports by the Nominated Officer are provided at a frequency that accords with the risk profile of the regulated business; and

(d) the institution has adequate policies and processes for screening prospective and existing staff to ensure high ethical and professional standards.

388. The Board must ensure that the institution's AML/CFT/CPF policies and procedures are effectively implemented. This means:

(a) ensuring that front line, sensitive[159] and compliance functions are subject to enhanced oversight;

(b) ensuring the internal audit function assesses the risk management practices and internal controls of the institution including annually assessing the effectiveness of the institution's compliance with its AML/CFT/CPF policies and procedures;

(c) compliance and oversight functions are provided with adequate resources to ensure that AML/CFT/CPF policies and procedures are effectively implemented; and

(d) ensuring the external audit function annual engagement extends to the institution's compliance with its AML/CFT/CPF policies and procedures.

389. The Board must ensure it receives adequate and annual training on the local AML/CFT/CPF laws and framework as well as the international standards and best or sound practices which impact AML/CFT/CPF obligations for regulated entities.

EMPLOYEE INTEGRITY STANDARDS

390. Procedures should be in place to ensure high standards of integrity and a code of ethics for the conduct of employees; including the meeting of statutory "fit and proper" criteria of the officers[160] of the company.

391. The procedures should allow for regular reviews of employees' performance and their compliance with established rules and standards, as well as provide for disciplinary action in the event of breaches of these rules. They should also include paying attention to employees whose lifestyles cannot be supported by their salary. The procedures should expressly provide for special investigation of employees who are associated with mysterious disappearances or unexplained shortages of funds.

392. Compliance with AML/CFT/CPF procedures should be among the factors taken into account in the job review process of relevant employees and consideration should be given to conducting a personal, professional and financial background check of the candidate when considering their application.

---

[159] Sensitive functions include cash transactions, cash management functions, preparation of accounts, data input and analysis.

[160] "officer" in relation to a company, means a person who, in that company—

(a) is a director of the company, president or vice president, general manager, nominated officer, secretary, financial controller or treasurer; or

(b) performs functions similar to those normally performed by the holder of any position referred to in paragraph (a).

393. Employment policies should provide for the investigation and evaluation of the personal employment history of employees. All new employees should be subject to such investigation and evaluation.

394. Regulated businesses should establish a 'whistle-blower' policy, in order to facilitate an environment that allows persons to report breaches without fear of occupational detriment.

Know Your Employee

395. Potential candidates for employment should be subject to a comprehensive screening process, which should involve a thorough investigation of that candidate's employment, financial, credit and criminal history.

396. Regulated businesses are required to have policies and procedures that facilitate ongoing monitoring of an employee's-

(a) Competence to undertake the role or position to which the employee is assigned;

(b) Compliance with statutory obligations for example, income tax and professional standard requirements;

(c) General character;

(d) Compliance with the institution's policies and procedures;

(e) Adherence with ethical practices and conduct;

(f) Behaviours exhibited which accord with ethical and moral standards-behaviours in this category generally include:

(i) Propensity to be forthright;

(ii) Absence of, or prompt declaration of conflict of interest issues;

(iii) Absence of a culture of loophole mining (whether with internal policies or in relation to the institution's statutory obligations);

(iv) Culture of compliance (with internal policies and with the institution's statutory obligations;

(v) Absence of a tendency or propensity to lie, cheat, mishandle the institution's property, including borrowing without permission, stealing, handling the property recklessly or negligently.

397. Regulated businesses 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) Regular review of employee's performance and adherence to internal policies and procedures including codes of conduct and AML/CFT/CPF requirements;

(c) Imposition of appropriate disciplinary actions for breaches of the institution's AML/CFT/CPF policies and procedures;

(d) Imposition of appropriate disciplinary or other appropriate actions 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

(e) Close scrutiny and investigation of employees whose lifestyles cannot be supported by his or her known income.

Education And Training[161]

398. To ensure full implementation of the procedures, recommendations, and requirements contained in the Guidelines, the staff of regulated businesses must be made fully aware of the serious nature of AML/CFT/CPF activities. Furthermore, efforts must be made to ensure that all staff understand the basic provisions of the applicable legislation.

399. Regulated businesses must provide training to their employees to inform them of their AML/CFT/CPF responsibilities. The timing and content of training for 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. AML/CFT/CPF policies and procedures manual should be readily available to all employees for instance, ensuring:—

(a) such documents are available on internal electronic access (e.g. intranets);

(b) sufficient copies are placed in resource centres or in-house libraries; and

(c) 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.)

400. Training/education programmes must be designed and implemented on an ongoing basis by regulated businesses to ensure employees' awareness of:—

(a) Current as well as new and developing AML/CFT/CPF laws, regulations, standards and guidelines being established both locally and internationally;

(b) Their legal obligations and responsibilities to detect and prevent ML/TF/PF;

(c) New ML/TF/PF techniques, methods, typologies and trends;

(d) The institution's own AML/CFT/CPF policies and procedures, including proper identification, record-keeping, internal control and communication procedures.

---

[161] Regulation 6, POC-MLPR; Section 18, TPA.

401. Members of staff must be made aware of their obligations under the POCA, the TPA and the UNSCRIA as they can be held personally liable for failing to report relevant information to the Nominated Officer or the Designated Authority, or otherwise failing to carry out their responsibilities under the applicable legislation.

402. Under POCA, persons in the regulated sector can raise a defence of either not knowing/suspecting that another person is engaging in ML, or not being provided with the requisite training by the employer.[162] Under the TPA, a defence of having a reasonable excuse for not making a report in relation to assets held for listed entities or STRs, can be raised in relation to proceedings for an offence under section 15 or section 16. 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.

403. Compliance with this requirement to train employees is perhaps best achieved in systems that trigger automatic training requirements on the occurrences of certain events e.g.:

(a) Employment;

(b) Promotion/lateral movement to sensitive or frontline duties; or

(c) Expiration of minimum period since last training session, thereby triggering refresher-training requirements.

404. Training initiatives should not be confined to scheduled sessions but should include spontaneous initiatives within randomly selected areas of operation. A mixture of such processes is likely to result in a more robust system that can quickly reveal shortfalls for management's attention as against relying on a system that is confined to scheduled, standardized style of training.

405. In any event, all relevant employees are to be provided with AML/CFT/CPF training at least once per year.

406. Regulated businesses must maintain proper training logs for all AML/CFT/CFP training initiatives to ensure that satisfactory steps are taken to confirm that training of employees occurred. Such steps may include the following:

(a) Ensuring such sessions are subject to rigorous registration systems that require signing by trainees and true records of the training session documented and retained in formal training registers;

(b) Videotaping of scheduled training sessions. Seminar participants must be made aware that the session is being taped or recorded in any way;

(c) Delivery of documented certification to employees evidencing satisfactory completion of training session;

(d) Demonstration of knowledge retention of training material, for example, test scores;

(e) Separate verification of the training sessions having taken place by the nominated officer; and/or

(f) Sign off on the sessions taking place by the Board of the regulated business as a part of the audited annual report of the regulated business.

407. In developing education and training programmes,[163] particular attention should be given to the following categories of staff:

(a) New Employees: AML/CFT/CPF training must be provided prior to the commencement of customer facing/relevant activities.

(b) Front Line Employees: 'Front-line' staff members (such as Cashiers, Customer Service Representatives, and Receptionists) should be provided with specific training on the various typologies of suspicious transactions. 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 Employees: Employees who deal with account opening, or the approval of new customers must receive the same training provided to Front Line Employees. They must further be advised that a business relationship or 'one-off' transaction shall not be established or continued beyond 14 days until the identity of the customer is verified.

(d) Administration/Operations Supervisors and Managers: Instructions covering all aspects of AML/CFT/CPF 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, TPA and the UNSCRIA, the procedures relating to monitoring orders, production orders and other court orders, the requirements for non-disclosure and for retention of records, and management's specific responsibility with dealings with customers in accordance with the risk profiles applicable to those customers.

SECTION XI — SPECIAL GUIDANCE—TRUST AND CORPORATE SERVICE PROVIDERS (TCSPs)

408. This section specifically addresses firms, proprietors, directors, managers, Nominated Officers and employees of trust or corporate service providers as defined under the TCSPA.

409. In implementing FATF Recommendation 22, the Proceeds of Crime (Designated Non-Financial Institution) (Trust and Corporate Service Providers) Order, 2022, and the Terrorism Prevention (Reporting Entities) Order, 2022, were issued pursuant to powers conferred respectively on:

(a) the Minister of National Security pursuant to paragraph 1(2) of the Fourth Schedule to the POCA, and

(b) the Minister of Foreign Affairs and Foreign Trade pursuant to section 15 (2) of the Terrorism Prevention Act.

---

[162] Section 94(6), POCA.
[163] Interpretive Note to FATF Recommendation 18.

410. These Orders effectively designated trust and corporate service providers as non-financial institutions and reporting entities respectively for the purposes of detecting, preventing and reporting money laundering, terrorist financing and proliferation financing.

411. Pursuant to the TCSPA, all persons who provide trust and corporate services as a business must be licensed by the FSC and are therefore subject to these Guidelines.

412. Trust services[164] are:

(a) The creation of a trust;

(b) Acting as a trustee, executor or administrator in relation to the trust;

(c) Arranging for any person to act as trustee in respect of the trust;

(d) Administration services in relation to the trust;

(e) Any other service that the Minister may, by order published in the *Gazette*, prescribe as a trust service.

413. Corporate services[165] are:

(a) Acting as a coordinator or an assistant in the formation, management or administration of a firm or company;

(b) Acting as (or arranging for another person to act as) a director or secretary of a company, an alternate director or a partner of a firm;

(c) Providing a registered office, business address, correspondence address or administrative address, for a company or firm of for any other person;

(d) Acting as (or arranging for another person to act as) a nominee shareholder for another person;

(e) Arranging the establishment of any legal entities not covered by any of the foregoing paragraphs and providing any of the foregoing services to such entities; and

(f) Any other service that the Minister may, by order published in the *Gazette*, prescribe as a corporate service.

414. TCSPs are subject to all obligations imposed on regulated businesses, as mentioned above, save and except the requirement to file threshold transaction reports on cash transactions. TCSPs cannot legally conduct cash transactions exceeding $1 million.

415. In addition to the obligations imposed on TCSPs above, they are required to maintain a register of beneficial owners of their clients.

Maintain a Register of Beneficial Owners

416. Pursuant to section 16 (1) of the TCSPA, TCSPs are required to keep accurate business records that will enable the identification and verification of the ultimate beneficial owner(s) of their clients. A TCSP who acts as a trustee, is required under the Trusts Act, as amended in 2021 to keep or caused to be kept adequate accurate and current records in respect of the identity of the settlor, protector (if any), enforcer, a beneficiary or class of beneficiaries, trustee and any person who has effective control of the trust.

417. The register of beneficial owners pursuant to regulation 9 of the Trust and Corporate Service Providers (Licensing and Operations) Regulations, 2022 must contain the following information with respect to each beneficial owner:

(a) The full name of the individual;

(b) The date on which the individual became a beneficial owner;

(c) The date on which the individual ceased to be a beneficial owner, where applicable;

(d) A copy of a valid identification (including driver's licence, a passport or any other national identification);

(e) The residential address, and if different, an address for service of documents;

(f) Date of birth;

(g) Nationality;

(h) Occupation;

(i) Particulars of beneficial interest held;

(j) Taxpayer Registration Number or such other unique reference number.

418. The register of beneficial owners must be kept up to date. Therefore, whenever there is a change in the beneficial ownership of a client the register must be updated no later than three (3) days thereafter. A failure to update the register of beneficial owners amounts to an offence punishable by fine or imprisonment or both such fine and imprisonment.

Identifying the Beneficial Owner of Legal Persons

419. The POC-MLPR establishes a cascading method for the identification of beneficial owners of legal persons. The first step is to obtain and verify the identity of the natural persons who ultimately have a controlling ownership interest in a legal person (whether by shares, voting, property, or other rights).

---

[164] Section 15, TCSPA.
[165] Section 14, TCSPA.

420. If there is a doubt as to whether a person with controlling ownership interest is a beneficial owner, or where no natural person exerts control through ownership interests, then the second step is to identify a natural person exercising control of the legal person through other means, for example a Board of Directors.

421. Where no natural person(s) is/are identified using the aforementioned methods, the third and final step is to identify and take reasonable measures to verify the identity of the relevant natural person who holds the senior managing position.

Recordkeeping Requirements

422. Under regulation 14(5) of the POC-MLPR, each TCSP (including professional trustees) must maintain certain records (see Section IX for records to be maintained) for—

(a) A period of seven years commencing on the date on which the relevant financial business was completed, or the business relationship was terminated, whichever occurs later; or

(b) Such other period as may be specified in writing by the Designated Authority before the expiration of the 7-year period.

SECTION XII—CONCLUSION

423. The Guidelines serve to inform the FSC's regulated businesses of the minimum standards required for an effective programme to detect and deter ML/TF/PF. The AML/CFT/CPF policies and procedures of regulated businesses should be developed in accordance with the law and these Guidelines, giving consideration to each institution's risk profile, organizational structure, internal procedures and policies, and where applicable, the policies of the financial group in which the regulated business resides.

SECTION XIII—APPENDICES

APPENDIX I (A)—EXAMPLES OF UNUSUAL/SUSPICIOUS TRANSACTIONS FOR SECURITIES DEALERS

424. Certain Cash Transactions, for example—

(a) Cash transactions that are not consistent with the business activities of the customer.

(b) Increases in cash transactions of the customer without apparent cause, especially if such amounts 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 transactions by a customer whose business activities would normally be in the form of cheques and other instruments.

(d) A series of cash transactions by a customer, where each transaction is minimal, but the total is significant.

(e) The frequent conversion of cash by a customer into financial instruments e.g. drafts, money transfers or other negotiable and readily marketable money instruments.

(f) Large cash investments using depository facilities and avoiding direct contact with financial institution staff.

(g) Cash investments directly into personal accounts where source of funds indicate business proceeds.

425. Operation of Accounts, for example—

(a) The use of a number of trustee or client accounts, which do not appear consistent with the customer's type of business;

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

(c) Large number of individuals making payments into the same account;

(d) Large withdrawals/encashment from a previously dormant/inactive account, or from an account that has just received an unexpected large transfer;

(e) Where funds are merely passing through the account, in that, the investments are encashed almost immediately;

(f) Payment of large amounts to a third party;

(g) High account turnover inconsistent with the profile of the customer;

(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 account;

(i) A dormant account with a minimal sum suddenly receiving funds by wire transfer followed by daily cash withdrawals that continue until the transferred sum has been depleted;

(j) Multiple wire transfers from different senders particularly from high-risk jurisdictions and funds are either transferred or withdrawn immediately;

(k) Making multiple investments just below the threshold for source of funds information.

426. Investment Related Transaction, for example—

(a) Buying and selling of securities with no discernible purpose or in circumstances that appear unusual;

(b) Requests by customers for investment management services where the source of the funds is unclear or not consistent with the customers' financial position.

427. Off-Shore Financial Activity, for example—

(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) Regular payments by customers, including wire transfers, that cannot be clearly identified as *bona fide* transactions to, or receipt of regular payments from, countries which are commonly associated with the production, processing or marketing of drugs or ML, or which are regarded as tax havens.

(c) Unexplained electronic fund transfers by customers on an in-and-out basis.

428. 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.

APPENDIX I (B) - EXAMPLES OF MONEY LAUNDERING TYPOLOGIES IN THE INSURANCE SECTOR

429. Money laundering typologies in the insurance sector include—

(a) Cash purchase of a single premium product from an insurer followed by early cancellation. A customer may purchase a life insurance policy that has a large surrender value, paying for the premium in cash. Shortly after receiving the policy, he will encash it and request payment to be made by cheque, draft or wire transfer to him or third parties;

(b) General Insurance bought to cover an office building or warehouse complex owned by a launderer through a company. Through arson or other means, the launderer/company causes a claim to be made to recover under the insurance policy;

(c) Cash payments of premiums;

(d) Free Look (Cooling off Periods) allows for refunds of premiums within the contract cancellation period. A number of life insurance products give the customer a right to cancel the contract within a short period. The customer will then obtain a refund of the paid premiums with clean money;

(e) Collusion of Intermediary and/or Insurance Company. Several cases involved collusive conduct between either the customer and the intermediary or between the intermediary and the insurance company. The intermediaries accepted illicit funds and transferred them in exchange for high commissions;

(f) Third Party Payments of Premiums. In some cases, third parties who have not been subject to the regular identification procedures when the insurance contract was concluded will fund insurance policies. The source of funds and the relationship between policyholder and third party is unclear to the insurance company;

(g) Large lump sum payment to policy;

(h) Insurance product that is purchased has no identified purpose;

(i) Scale of investment in insurance policies is inconsistent with the client's financial profile;

(j) Use of life insurance product in a manner resembling use of a bank account, that is, making additional premium payments and frequent partial redemptions;

(k) Repeated and unexplained changes in beneficiary;

(l) Relationship between the policyholder and the beneficiary is unclear.

APPENDIX I (C)—EXAMPLES OF MONEY LAUNDERING TYPOLOGIES IN THE TCSP SECTOR

430. The following are examples of ML typologies in the TCSP sector:

(a) The formation of shell companies by TCSPs that can be used by money launderers;

(b) The operation of virtual overseas offices which provide TCSP services;

(c) The use of nominee agreements to hide from the TCSP the beneficial ownership of client companies;

(d) The use of foreign private foundations that operate in jurisdictions with secrecy laws;

(e) Transactions that utilize complex and opaque legal entities and arrangements;

(f) Multiple trust accounts with same beneficiary;

(g) Trust account receiving multiple cash deposits;

(h) Transactions in trust account are inconsistent with customer profile;

(i) The use of TCSPs as nominee shareholder to obscure beneficial ownership of legal person.

APPENDIX II—CONSEQUENCES OF NON-COMPLIANCE

431. All regulated entities can ensure compliance with the provisions of the AML/CFT/CPF legislation by adopting control procedures such as those outlined in the Guidelines, and such procedures should be documented and reviewed from time to time, as appropriate. In determining whether a person has complied with the provisions of the AML legislation, (Regulation 3(3) and (4) of POC-MLPR, 2007), the TPA legislation, (Regulations 3(1) and 3(2) of TP-RER,), or the UNSRCI-RER (Regulations 3(1) and 3(2), the court is required to take account of relevant Guidelines and consider whether the regulated business took all reasonable steps and exercised due diligence to comply with the law. Section 18(4) of the TPA and Regulation 5(4) of POC-MLPR direct regulated businesses to consult with the Competent Authority for the purpose of carrying out their obligations under Section 18, (Regulatory Controls by Certain Entities) of the TPA and POC-MLPR respectively.

432. Failure to comply with the provisions of the law may result in the following consequences—

(a) Criminal Prosecution—There are penalties for breaches of the provisions of the ML/TF/PF prevention legislation, whether by firms, individuals or employees;

(b) Commercial Losses—The institution may incur non-productive costs to address issues arising out of investigations into alleged ML/TF/PF activities, costs to defend prosecutions, and costs and costs to repair the institution's public image;

(c) Loss of Reputation—Institutions that, even inadvertently, become involved in ML/TF/PF activities risk loss of their good name in the market. This may occur because of media coverage of the circumstances.

TABLE 8—SCHEDULE OF OFFENCES AND PENALTIES (POC LEGISLATION)

Offences Under POC Legislation	Individual Sanctions	Body Corporate Sanctions
Engaging in transaction that involves criminal property (Section 98)	Up to 5 years in prison and/or J$3M (Parish Court Court); Up to 20 years in prison and/or a fine (Circuit Court)	Fine up to J$5M (Parish Court); A fine (Circuit Court)
Concealing, disguising, disposing of or bringing into Jamaica criminal property (Section 98)	Up to 5 years in prison and/or J$3M (Parish Court); Up to 20 years in prison and/or a fine (Circuit Court)	Fine up to J$5M (Parish Court); A fine (Circuit Court)
Converting, transferring, or removing criminal property from Jamaica (Section 98)	Up to 5 years in prison and/or J$3M (Parish Court); Up to 20 years in prison and/or a fine (Circuit Court)	Fine up to J$5M (Parish Court); A fine (Circuit Court)
Facilitating the acquisition, retention, use or control of criminal property by or on behalf of another (Section 98)	Up to 5 years in prison and/or J$3M (Parish Court); Up to 20 years in prison and/or a fine (Circuit Court)	Fine up to J$5M (Parish Court); A fine (Circuit Court)
Acquiring, using or having possession of criminal property (Section 98)	Up to 5 years in prison and/or J$3M (Parish Court); Up to 20 years in prison and/or a fine (Circuit Court)	Fine up to J$5M (Parish Court); A fine (Circuit Court)
"Tipping off"—Unauthorized Disclosures about money laundering investigation being or to be conducted by the enforcing authority (Section 104)	Up to 12 months in prison and/or up to a fine of J$1M (Parish Court); Up to 10 years in prison and/or a fine (Circuit Court)	N/A
"Tipping off"—Unauthorized Disclosures about a Report under section 100 of the Act (Section 98)	Up to 12 months in prison and/or up to a fine of J$1M (Parish Court); Up to 10 years in prison and/or a fine (Circuit Court)	N/A
Failure to make required disclosure (Suspicious Transaction Reports) to the Nominated Officer or the Designated Authority (Section 98)	Up to 12 months in prison and/or up to a fine of J$1M (Parish Court); Up to 10 years in prison and/or a fine (Circuit Court)	N/A
Failure by the Nominated Officer to make required disclosure (Suspicious Transaction Reports) to the Designated Authority (Section 98)	Up to 12 months in prison and/or up to a fine of J$1M (Parish Court); Up to 10 years in prison and/or a fine (Circuit Court)	N/A

TABLE 8—SCHEDULE OF OFFENCES AND PENALTIES (POC LEGISLATION), *contd.*

Offences Under POC Legislation	Individual Sanctions	Body Corporate Sanctions
Failure by the Nominated Officer to act in accordance with the law when giving appropriate consent to the doing of a prohibited act (Section 99)	Up to 12 months in prison and/or up to a fine of J$1M (Parish Court); Up to 5 years in prison and/or a fine (Circuit Court)	N/A
Failure to carryout identification procedures, transaction verification procedures, record keeping procedures of internal control and communication, required training. [Reg. 6(2)]	Up to 3 years in prison and/or up to a fine of J$3M (Parish Court); Up to 20 years in prison and/or a fine (Circuit Court)	Fine up to J$5M (Parish Court); A fine (Circuit Court)
Failure to establish and implement such programmes, policies, procedures and controls as may be necessary for the purpose of preventing or detecting money laundering— namely: ensuring high standards of integrity of employees; evaluating personal employment and financial history of employees; training of employees; arranging independent audit; and selecting a Nominated fficer. [Reg. 5(5)]	Up to 3 years in prison and/or up to a fine of J$3M (Parish Court); Up to 20 years in prison and/or a fine (Circuit Court)	A fine of up to $5M (Parish Court) A fine (Circuit Court)
Failure to include in its records accurate and relevant information on electronic funds transfers. [Reg. 9(3)]	Up to 3 years in prison and/or up to a fine of J$3M (Parish Court); Up to 20 years in prison and/or a fine (Circuit Court)	A fine (Circuit Court)
Failure to file Threshold Transaction Reports ("TTR") with Designated Authority; Breach of duty of non-disclosure; Failure to comply with directions of the Designated Authority re TTRs and STRs [Reg. 3 (7)]	N/A	A fine of up to J$1M (Parish Court)
Failure of a branch/subsidiary of a regulated entity to comply with Part V of POCA and POC-MLPR or the higher of the required standard between the jurisdictions where the regulated business is located and that which the branch/ subsidiary is located. [Reg. 18(3)]	Up to 3 years in prison and/or up to a fine of J$3M (Parish Court); Up to 20 years in prison and/or a fine (Circuit Court)	A fine of up to J$5M (Parish Court) A fine (Circuit Court)
Regulated entities failing to notify the Competent Authority of its branch/subsidiary inability to comply with Part V of POCA and POC-MLPR. [Reg. 18(3)]	Up to 3 years in prison and/or up to a fine of J$3M (Parish Court); Up to 20 years in prison and/or a fine (Circuit Court)	A fine of up to J$5M (Parish Court) A fine (Circuit Court)
Failure to comply with requirement or direction issued by the Competent Authority (section 91A (5)	N/A	A fine up to $3M (Parish Court) A Fine (Circuit Court)

TABLE 8—SCHEDULE OF OFFENCES AND PENALTIES (POC LEGISLATION), *contd.*

Offences Under POC Legislation	Individual Sanctions	Body Corporate Sanctions
Failure to implement enhanced measures in respect of transactions with customers domiciled, resident or incorporated in specified territories. (Section 94A(3))	N/A	A fine up to $3M (Parish Court) A Fine (Circuit Court)
Breach of declaration provision of cross border movement of funds (Section 101)	A fine up to J$250,000 or 3 times the cash being transported (whichever is greater) and/or up to 3 months in prison (Parish Court)	
Breach of Reg. 7 (Identification procedures, business relationships and transactions procedures)	A fine of up to J$5M (Parish Court) A fine (Circuit Court)	
Breach of Reg. 7A (Establishment of risk profiles and ongoing due diligence verification procedures)		
Breach of Reg. 7B (Enhanced money laundering counter-measures)		
Breach of Reg. 11 (Identification procedures for agent)		
Breach of Reg. 14 (Recordkeeping procedures)		
Breach of Reg. 15 (Internal Reporting procedures)		
Breach of Reg. 16 (Prohibition on operating anonymous, fictitious or numbered account)		
Breach of Reg. 17 (Use of prescribed reporting form) [Reg. 20]		

TABLE 9—SCHEDULE OF FIXED PENALTIES—SECOND SCHEDULE—POC-MLPR

Regulation	Offence	Fixed Penalty
5(5)	Failure to comply with the regulation 5(1) requirement to establish and implement programmes, policies, procedures and controls necessary for the purpose of preventing or detecting ML	
5(5)	Failure to comply with regulation 5(3)—requirement tonominate an employee to be responsible for implementing programmes etc.	
6(2)	Non-compliance with regulation 6(1) in forming a business relationship or carrying out a one-off transaction.	Individual—J$2.1 million
18(3)	Failure to comply, implement and conform with, or advise of inability to conform with, etc., standards and conduct set out in Part V of the Act and in the Regulations.	Body Corporate—J$3.5 million
20(1)	Failure to comply with regulation 7—requirements regarding identification and transaction verification procedures, etc.	
20(1)	Failure to comply with regulation 7A—requirements to establish risk profiles and carry out due diligence.	
20(1)	Failure to comply with regulation 11—requirements regarding identification procedures concerning transactions carried out by agents.	
20(1)	Failure to comply with regulation 14—record-keeping requirements	
20(1)	Failure to comply with regulation 15—requirements for internal reporting procedures.	
20(1)	Failure to comply with regulation 16—prohibition on conducting transaction by means of numbered accounts, anonymous accounts or accounts in fictitious names.	
20(1)	Failure to comply with regulation 17—requirements as to form of reports.	

TABLE 10—OFFENCES AND PENALTIES: TERRORISM PREVENTION LEGISLATION

Offences Under the Terrorism Prevention Legislation	Individual Sanctions	Body Corporate Sanctions
Failure to report to the Designated Authority whether or not the institution is in possession or control of property owned or controlled by or on behalf of a listed company [Section 15(7)]	Up to 12 months in prison and/or J$1M (Parish Court)	Fine up to J$3M (Parish Court)
Unauthorized disclosure of report on listed entities made to Designated Authority [Section 15(7)]	Up to 12 months in prison and/or J$1M (Parish Court)	Fine up to J$3M (Parish Court)
Failure to report suspicious transactions to the Designated Authority [Section 16(4)]	Up to 12 months in prison and/or J$1M (Parish Court)	Fine up to J$3M (Parish Court)
Unauthorized disclosure re: investigation of terrorism offence by the Designated Authority and Terrorism Reports made to the Nominated Officer and the Designated Authority [Section 17(5)]	Up to 2 years in prison and/or J$2M	Fine up to J$6M
Failure to implement regulatory controls [Section 18(6)]	N/A	A fine of up to J$1M (Parish Court)
Failure to comply with any direction or requirement issued by the Competent Authority [section 18A(5)]	N/A	Fine up to J$3M (Parish Court) Fine (Circuit Court)
Failure to implement appropriate procedures to prevent TF (Reg. 4(2))	Up to 12 months in prison and/or fine up to J$1M (Parish Court)	Fine up to J$3M (Parish Court)
Failure to comply with requirements pertaining to electronic funds transfers (Reg. 9(3))	Up to 12 months in prison and/or fine up to J$1M (Parish Court)	Fine up to J$3M (Parish Court)
Failure to apply standards to overseas branches and subsidiaries (Reg. 18(4))	Up to 3 years in prison and/or fine up to J$3M (Parish Court) Up to 20 years in prison or fine (Circuit Court)	Fine up to J$1M (Parish Court) Fine (Circuit Court)
Failure to comply with directions from the designated authority (Reg. 19(3))	Up to 12 months in prison and/or fine up to J$1M (Parish Court)	Fine up to J$3M (Parish Court)

TABLE 11—OFFENCES AND PENALTIES: UNSCRI LEGISLATION

Failure to submit prescribed reports to the designated authority (Section 3 (7))	Up to 6 months in prison and/or J$500,000 (Parish Court)	Fine up to J$3M (Parish Court)
Contravention of Section 8A—Prohibition from dealing with assets of proscribed person (Section 8A(3))	Fine or life imprisonment	N/A
Failure to comply with directions issued by the designated authority (Reg. 8(3))	Up to 3 years in prison and/or fine up to J$3M (Parish Court)	Fine up to J$5M (Parish Court)
Failure to comply with any requirement or direction issued by the competent authority (Reg. 9(4))	N/A	Fine up to J$3M (Parish Court) Fine (Circuit Court)

PRINTED BY JAMAICA PRINTING SERVICES (1992) LTD., (GOVERNMENT PRINTERS), DUKE STREET, KINGSTON, JAMAICA