THE

JAMAICA GAZETTE

EXTRAORDINARY

704G[1]

Vol. CXLIII **FRIDAY, SEPTEMBER 25, 2020** **No. 198C**

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

RYAN EVANS
Governor-General's Secretary and
Clerk to the Privy Council.

GOVERNMENT NOTICE

No. 216E

MISCELLANEOUS

THE BETTING GAMING AND LOTTERIES GUIDELINES ON THE DETECTION AND PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCING OF TERRORISM AND PROLIFERATION

Guidance for Gaming Machine Operators on gaming lounge premises

Explanatory Forward

These Guidelines have been updated to incorporate the amendments to the Anti-Money Laundering (AML) and Counter Financing of Terrorism (CFT) legislation, the passage of the United Nations Security Council Resolutions Implementation Act, and the revised Financial Action Task Force (FATF) Forty (40) Recommendations and Guidance. The Betting, Gaming and Lotteries Commission (BGLC) as the Competent Authority has the responsibility for ensuring that its licensees are compliant with respect to their AML/CFT and counter proliferation financing (CPF) requirements under prescribed legislation.

Consequently, these Guidelines provide gaming machine operators with new measures to be implemented. These measures include the requirement to adopt a risk-based approach to their respective AML/CFT/CFP framework; develop risk profiles for all customers with corresponding Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements; a heightened focus on Politically Exposed Persons (PEPs).

This document supersedes the Betting, Gaming and Lotteries Commission- Anti-Money Laundering Guidance Notes for Gaming Lounge Operators issued on January 26, 2016.

PART 1—*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, (UN Act);

The United Nations Security Council Resolution Implementation (Asset Freeze -Democratic

People's Republic of Korea) Regulations;

The United Nations Security Council Resolution Implementation Regulations;

The Betting, Gaming and Lotteries Act (BGLA);

The Financial Investigations Division Act;

The Companies Act;

The Revenue Administration Act;

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

"AML" means anti-money laundering

"business relationship" means any arrangement between two or more persons where the purpose of the arrangement is to facilitate:

(a) the carrying out of more than one transaction between the persons concerned; or

(b) the carrying out of transactions between the persons concerned on a frequent, habitual or regular basis.

"cash transaction" means a transaction involving the physical transfer of currency from one person to another.

"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 and terrorism financing.

"criminal spend" means the use of the proceeds of crime to fund gambling as a leisure activity.

"customer" means a person seeking to form a business relationship, or to carry out a one-off transaction with a business in the regulated sector.

"customer due diligence" means the care that a person should take before entering into a transaction with another person. It includes, establishing the identity of the customers, monitoring account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account.

"currency" means the coin and bank notes designated as the legal tender of Jamaica, or any other foreign country.

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

"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 of National Security as a non-financial institution;

"designated non-financial business and profession (DNFBP)" means the same as "designated non-financial institution (DNFI)".

"DPP" means Director of Public Prosecution

"entry" means the beginning of either a one-off transaction or a business relationship.

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

"freezable assets" means an asset that is:

(a) is owned or controlled by an entity designated in Annex I or Annex II of Resolution 2087 found within the United Nations Security Council Resolution Implementation (Asset Freeze-Democratic People's Republic of Korea) Regulations, 2013; or

(b) is derived or generated from any asset mentioned in paragraph (a).

"gaming machine operator(s)' means-a person who operate twenty or more gaming machines on any prescribed premises under a licence issued by the Betting, Gaming and Lotteries Commission pursuant to the Betting, Gaming and Lotteries Act ("BGLA').

"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, where a person:

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

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

(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 nominated by a regulated business who performs management functions and has responsibility for the establishment, implementation and maintenance of the system to detect and prevent (ML/FT/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 licensees to give specified information and documents to a named constable.

"one-off transaction" means any transaction carried out other than in the course of a business relationship.

"permitted persons" has the meaning assigned in Section 101A(6) of the POCA.

"person" means an individual or a legal entity.

"Prescribed premises'' means a gaming lounge with twenty or more gaming machines licensed as a Prescribed premises (hotel) or Prescribed Premises (gaming lounge)

"principal" includes beneficial owners, settlers, controlling shareholders, directors and major beneficiaries.

"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.

"regulated entity" means a licensee or a DNFI which falls under the provisions of POCA, TPA and UN Act.

"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 UN Act.

"specified offence" means an offence listed under the Second Schedule of POCA

"suspicious transactions" means complex, unusual or large business transactions, or unusual patterns of transactions whether completed or not, which appear to the regulated entity to be inconsistent with the normal transactions carried out by that customer with the institution.

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

"transaction" refer to all curency transfer including cash-in and cash-out of a gaming machine operator.

"Assets" means:

(a) Property of any kind

i. whether tangible or intangible, movable or immovable, however acquired; and

ii. owned wholly or jointly, directly or indirectly, by a person or entity proscribed under section 3 (2)(a) of the UNSCRIA or by a person or entity acting on behalf of, or at the direction of, a person or entity proscribed under section 3(2)(a) of the Act; or

(b) a legal document or instrument in any form, including electronic or digital, evidencing title to, or interested in, property as described in paragraph (a), including (but not limited to) bank credits, traveller's cheques, bank cheques, money orders, shares, securities, bonds, debt instruments, drafts and letters of credit.

"Customer Information" includes:

(a) the applicant for business' full name, current address, taxpayer registration number (TRN) or other reference number, date and place or birth and mother's maiden name (in the case of an individual) and, where applicable, the information referred to in regulation 13(1)(c) of the POC (MLP) Regulation;

(b) any other information used to verify the applicant for business' identity or the nature of the applicant for business' trade, profession or source of funds.

Objectives

1. These Guidance Notes have been issued pursuant to section 91(g)(ii) of the POCA and pursuant to Regulation 20(b) of the TP (Reporting Entities) Regulations 2010. The objective of these Guidance Notes is to inform gaming establishments that are subject to the supervision of the BGLC (in its capacity as Competent Authority) of their responsibilities under the applicable legislation, as well as to identify best practices in-AML, CFT and CFP procedures and systems.

2. The Guidelines first came into effect on January 26, 2016.

3. The Guidelines were amended to reflect the provisions of the POCA (Amendment) Act 2019, POC (MLP) (Amendment) Regulations 2019, the Terrorism Prevention (Amendment) Act, 2019, the Terrorism Prevention (Reporting Entities) (Amendment) Regulations, 2019, Resolution, the UNSCRIA 2013, UNSCRI (Amendment) Act, 2019 and the UNSCRI (Reporting Entities) Regulations 2019.

4. The Guidelines will be continuously reviewed and amended as necessary, to ensure its continued usefulness, efficacy, relevance and adherence to international best practice and to reflect any legislative amendment.

Applicability of these Guidelines

5. These Guidelines are applicable to all gaming machine operators classified as DNFI as defined by POCA, TPA and the UN Acts, which are regulated by the BGLC within the regulatory ambit of the Betting, Gaming and Lotteries Act.

6. The Guidelines are informed by:

(a) The Applicable Legislation;

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

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

7. The Guidelines along with the applicable legislation will form the framework against which the BGLC will assess the adequacy and effectiveness of the regulated entity's AML/CFT/CPF programmes.

Legal Status of these Guidelines

8. The Betting, Gaming and Lotteries Commission (BGLC) regulate and supervise gaming machine operators on prescribed premises (hotels and gaming lounge) in connection with gambling or other services as the Minister with responsibility for finance may direct.

9. On April 1, 2014, the BGLC was designated the **"Competent Authority"** under POCA by the Minister of National Security to supervise gaming machine operators in their responsibilities under POCA and POC-MLPR.

10. Effective May 2018, the BGLC was designated the **"Competent Authority"** under TPA by Order affirmed in the House of Representatives on November 29, 2017 by the Minister of Finance.

11. On November 15, 2013, the Minister of National Security, by Order, designated any person who operates twenty (20) or more gaming machines (gaming lounge) pursuant to a licence under the Betting, Gaming & Lotteries Act as a DNFI for the purposes of POCA and POC-MLPR.

12. On October 13, 2017, the Terrorism Prevention (Designated Reporting Entity) (Gaming Machine Operators) Order, 2017 was affirmed in the Senate and is applicable to any person who operates twenty (20) or more gaming machines (gaming lounge) pursuant to a licence under the Betting, Gaming & Lotteries Act.

13. Under Section 91(l)(g) of the POCA, Regulation 20(b) of the Terrorism Prevention (Reporting Entities) Regulations and Regulation 9 of The United Nations Security Council Resolutions Implementation (Reporting Entities) Regulations, the Competent Authority is required to issue guidelines to businesses in the regulated sectors regarding effective measures to prevent money laundering and terrorism financing respectively and to monitor the compliance of its regulated entities.

14. Under Section 91A of POCA, Section 18A of the TPA, and Section 9 of the UNSCRIA, 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; and the directions may require the business to take measures for the prevention or detection of, or reducing the risk of, money laundering or terrorist financing;

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 under the relevant Acts and subject to any terms, conditions or undertakings which it thinks fit in order to prevent disclosure.

e. is required to maintain statistical records, as it considers appropriate, for the purpose of measuring the overall effectiveness of measures taken with respect to the prevention of money laundering and terrorism financing. The Competent Authority also has the power to disclose to any authorized entity listed within sections 137A (4) and 18B (4) the statistical information it has recorded, if the information does not include any information from which the identity of a person, or any personal details in respect of any person, is ascertainable either on the face of the disclosure or by reasonable inference.[1]

---

[1]Section 137A the Proceeds of Crime (Amendment) Act, 2019 and Section 18B(4) of the Terrorism Prevention (Amendment) Act, 2019

f. may require the businesses concerned, in accordance with such procedures as it may establish by notice in writing to those businesses to make such reports to the competent authority in respect of such matters as may be specified in the notice.

15. Pursuant to POCA, POC-MLPR, the TP-RER and the UNSCRI-RER, a Court will take notice of these Guidelines, when considering whether a person commits an offence under POCA, TP-RER or UNSCRI-RER.

16. The relevant provisions are:

POCA

Section 94(7)(a):

In deciding whether a person committed an offence under this section or section 95 the Court shall consider whether the person followed:

(a) any relevant guidance that was at the time concerned:

i. issued by a supervisory authority or any other body that regulates, or is representative of any trade, profession, business or employment carried on by the alleged offender;

ii. approved by the Minister; and

iii published in the Gazette.

POC-MLPR

Regulation 2(3):

In determining whether a person has complied with any of the requirements of these Regulations, a court shall take account of any relevant guidance that was at the time concerned:

(a) issued by the designated authority or a body that regulates, or is representative of any trade profession, business or employment concerned;

(b) approved by the Minister; and

(c) published in the Gazette.

Regulation 2(4):

In proceedings against any person for an offence under this regulation, it shall be a defense for that person to show that he took all reasonable steps and exercised due diligence to avoid committing the offence.

Regulation 2(5):

In this regulation "supervisory or regulatory guidance" means guidance issued, adopted or approved by the relevant Competent Authority.

TP-RER

Regulation 3(1):

In determining whether a person has complied with any of the requirements of these Regulations, a court shall take account of any relevant guidance that was at the time concerned issued by the designated authority, competent authority or a body that regulates, or is representative of, any trade profession, business or employment concerned:

(a) with the approval of the Minister; and

(b) published in the Gazette.

Regulation 3(2):

In proceedings against any person for an offence under these Regulations, it shall be a defence for that person to show that he took all reasonable steps and exercised due diligence to avoid committing the offence.

UNSCRI-RER

Regulation 3(1):

In determining whether a person has complied with any of the requirements of these Regulations, a court shall take account of any relevant guidance that was at the time concerned issued by the designated authority, competent authority or a body that regulates, or is representative of, any trade profession, business or employment concerned:

(a) with the approval of the Minister; and

(b) published in the Gazette.

Regulation 3(2):

In proceedings against any person for an offence under these Regulations, it shall be a defence for that person to show that he took all reasonable steps and exercised due diligence to avoid committing the offence.

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

18. Failing to adhere to these Guidelines could result in:

i. An entity, its principals and/or its officers being deemed unfit to conduct business under the relevant sector legislation;

ii. A court holding that the gaming machine operator has not complied with the applicable legislation.

19. A conviction for an offence under any of the applicable legislation can adversely impact a person's ability to be deemed as 'fit and proper' and to continue to operate within the gaming industry.

PART IA—*Background*

Money Laundering

20. The term *'money laundering'* refers to all processes, methods, and transactions designed to change the characteristics of illegally obtained money so that it appears to have originated from a legitimate source. There are usually three fundamental stages of money laundering: placement, layering, and integration. Where all stages are achieved, they occur in sequence but there is often some overlap of the stages.

21. There is potential for the money launderer to use gaming at every stage of the process. The land-based gaming industry is particularly vulnerable during the placement stage as the use of cash is prevalent and the origin of such cash is not always easy to determine. Although customers utilize electronic payment methods such as debit/credit cards; identity theft and identity fraud can enable the money launderer to move criminal proceeds.

22. 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 Standards - 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 non-financial institution has the 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[2].

Terrorism Financing

23. 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.

24. Gaming machine operators should also be aware that business relationships with terrorists and terrorist organizations can expose the entity to significant legal, operational and reputation risks.

25. Gaming machine operators are placed under statutory obligations to ensure that they take active, effective and ongoing steps to prevent and detect terrorist financing[3]. 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.

26. Any gaming machine operator that carries out transactions, knowing that the funds or property involved are owned or controlled by terrorists or terrorist organisations, or that the transaction directly or indirectly linked to, or likely to be used in, terrorist activity, may be committing a criminal offence, and such an offence in many instances may exist regardless of whether the assets involved in the transaction were derived from unlawful activity.

27. Unlike money laundering, funds can come from both legal sources as well as from criminal activity. Funds may involve low dollar value transactions and give the appearance of legitimacy and a variety of sources such as personal donations, profits from businesses and charitable organizations e.g., a charitable organization may organize fundraising activities believing that the funds will go to relief efforts abroad, but, all the funds are actually transferred to a terrorist group.

28. Offences also include the financing of travelling expenses of an individual to another jurisdiction for the purpose of the perpetration, planning or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.

29. Section 46 of the TPA also provides that for the purpose of conferring jurisdiction, any offence committed outside of Jamaica shall be deemed to have been committed in Jamaica where the offender may be domiciled for the time being in Jamaica, if such offence, when committed in Jamaica, would have been a terrorism offence.

30. A key issue for gaming machine operators, 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, gaming machine operators 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 on an account over time.

Proliferation Financing

31. 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.

32. FATF Standards-Recommendation 7 requires countries to implement proliferation financing-related Targeted Financial Sanctions (TFS) made under United Nations Security Council Resolutions (UNSCRs). FATF Standards-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).

33. The 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 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 also 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.

---

[2]See Regulation 5 of POC (MLP) Regulations
[3]Section 18 TPA

(b) country-specific approach under UNSCR 1718 (2006) and UNSCR 2231 (2015) and their (future) successor resolutions-resolutions against the Democratic People's Republic of Korea (DPKR)[4] and the Islamic Republic of Iran.

34. 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.

35. Gaming machine operators are required to immediately freeze the funds, other financial assets and economic resources that are under their control at the date of the adoption or at any time thereafter, that are owned or controlled, directly or indirectly by the designated persons/entities. Additionally, gaming machine operators are to ensure that no funds or other assets or economic resources are made available to such persons and entities, except in specific situations, and under conditions specified in the UNSCRs.

36. The FATF Standards do not require countries to assess their proliferation financing risks, as the requirement to apply targeted financial sanctions in accordance with FATF Standards—Recommendation 7 is not risk-based but rules-based[5].

37. Section 3 of the UN Act allows the Minister, subject to affirmative resolution, to make regulations to give effect to decisions: of the Security Council under Chapter VII of the Charter; and which Article 25 of the Charter requires Jamaica to carry out any or all of the following means:

(a) proscribing persons or entities;

(b) restricting or preventing the supply, sale or transfer of goods or services;

(c) restricting or preventing uses of, dealings with, and making available, assets;

(d) restricting or preventing the procurement of goods or services;

(e) providing for indemnities for acting in compliance or purported compliance with those regulations;

(f) providing for compensation for owners of assets; and

(g) authorizing the making of legislative instruments.

Mutual Legal Assistance

38. The United Nations Resolution 1373 and the revised FATF Recommendations (R.36-40) require that states must have the ability to provide mutual assistance to each other, whether through the exchange of information, or facilitating the freezing and forfeiture of assets used to aid the commission of a terrorist offence in another jurisdiction. In Jamaica, the Mutual Assistance (Criminal Matters) Act of 1995, The Sharing of Forfeited Property Act of 1999, the Maritime Drug Trafficking (Suppression) Act of 1998 , the Interception of Communications Act of 2002, and the Extradition Act of 1991 permit Jamaica to extend assistance to other countries that are in the process of prosecuting, or enforcing judgments or forfeiture proceedings for a range of offences including drug related, revenue, money laundering and terrorist offences.

PART 2 —*AML/CFT/CFP Legislative and Regulatory Framework*

Applicable Legislation

The Proceeds of Crime Act (POCA)

39. POCA came into effect on the 30th of May 2007 and repealed and replaced the Money Laundering Act, 1998 ('MLA') and the Drug Offences (Forfeiture of Proceeds) Act, 1994 ('DOFPA').

40. 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. Criminal property[6] is any property that constitutes a benefit derived wholly or partially from criminal conduct. Criminal conduct[7] means any conduct constituting an offence in Jamaica, or if committed outside, conduct that would constitute a crime in Jamaica.

41. POCA comprises of 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.

---

[4]The United Nations Security Council Resolutions Implementation (Asset-Freeze-Democratic People's Republic of Korea) Regulations, 2013 was passed in November 2013.
[5]See FATF Guidance on Counter Proliferation Financing, February 2018.
[6]Section 91(1), POCA
[7]Section 91(2), POCA

(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 to note:

Offences under Part V (Money Laundering):

42. Section 92 (1) creates an offence where a person:—

i. engages in a transaction that involves criminal property[8]; or

ii. conceals, disguises, disposes of, or brings into Jamaica, criminal property[9]; or

iii. converts or transfers or removes criminal property from Jamaica,

if that person knows or has reasonable grounds to believe at the time, he does any act referred to at (a) (b) or (c), that the property is criminal property[10].

43. Gaming machine operators should note that willful blindness on the part of the person charged with the offence cannot be used as a defence.

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

- Conceals criminal property (for example, by depositing funds obtained through criminal activity into a gaming account);
- Disguises criminal property (for example, by placing funds obtained through criminal activity into a gaming account and then withdrawing them at a later date);
- Converts criminal property (for example, by placing bets in a gaming establishment and then cashing in the winnings);
- Transfers criminal property (for example, by transferring property to another person or to a gaming operator);
- Removes criminal property from Jamaica (for example, by taking his winnings overseas)[11].

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

46. Gaming machine operators should ensure that their terms and conditions with customers and contractual arrangements entered into in the course of the regulated business allows for the legal termination of the transaction, arrangement or business relationship if there is reasonable grounds that criminal activity is taking place which would expose that gaming establishment to legal or reputational risks due to the suspected criminal activity.

47. Section 93 (1) of the POCA makes it an offence where a person acquires, uses or has possession of criminal property and the person knows or has reasonable grounds to believe that the property is criminal property (for example, via stakes).

48. Section 94(2) makes it an offence for failing to make the requisite disclosure within the stipulated time frame *i.e. within 15 days after the information or matter comes to a person's attention* (s. 94 (2)(c)) in circumstances where there is knowledge or belief that another person has engaged in a transaction that could constitute or be related to money laundering (s. 94(2)(a)), and this knowledge or belief arose in the course of a business in the regulated sector (s.94(2)(c)); (Suspicious Transaction Report ('STR') obligation).

49. Section 95 makes it an offence where there is a failure of the nominated employee to make the requisite disclosure within the stipulated time frame *i.e. within 15 days after the information or matter comes to the nominated employee's attention* in circumstances where there is knowledge or belief on the part of the nominated employee that another person has engaged in a transaction that could constitute or be related to money laundering, and this knowledge or belief arose in the course of a business in the regulated sector; (STR obligation).

50. Section 97 makes each of the following matters a 'tipping off' offence (i.e. Offences of tipping off about a money laundering disclosure, tipping off about a money laundering investigation and prejudicing money laundering investigations)—

i. Disclosing information with the knowledge or belief that a protected or authorized disclosure has been made or is to be made under section 100, where such disclosure is likely to prejudice any investigation that might be conducted following the statutory disclosure, (s. 97)(l)(a). Disclosures in this regard refer to disclosures by regulated businesses (via nominated employee regime) and disclosures to an authorized officer (refer to section 100(4)(a);

ii. Disclosing information or any other matter with the knowledge or belief that the Agency, the DPP, or an authorized officer as defined by section 103 of the POCA, is acting or proposing to act in connection with a money laundering investigation that is being, or is about to be conducted (s. 97)(l)(b).

51. 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;

---

[8]Section 92(1)(a), of the POCA
[9]Section 92(1)(b), of the POCA
[10]Section 92(1)(c), of the POCA

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

52. Section 101 makes it an offence for 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.[12]

53. Section 101A places a restriction on cash transactions exceeding J$l million for the purchase of any goods or services or for the payment or reduction of any indebtedness, accounts payable or other financial obligation excepting for payments made to or by a permitted person, an exempted person or for an exempted transaction. Additionally, a person is prohibited from artificially structuring a cash transaction so that it falls below the prescribed amount where the aggregate would exceed that amount.

54. Specific areas of concern under POCA Part VI— Investigations

Offences are contained in sections 104 (2), 112,122,123.

55. 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.[13]

56. Failure without reasonable excuse to comply with a disclosure order[14]

57. Failure by a gaming machine operator without reasonable excuse, to comply with a customer information order.[15]

58. A gaming machine operator making a statement that it knows is false or misleading in a material particulars.[16]

59. A gaming machine operator recklessly making a statement that is false or misleading in a material particulars.[17]

60. 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 Jamaica Constabulary Force; Customs; the Competent Authorities, and any other person designated by the Minister. The BGLC as the Competent Authority, is responsible for monitoring compliance with the obligations of the POCA for its regulated entities.

61. Table: Areas of Enforcement under POCA and POC (MLP) Regulations

Areas of Enforcement	Act or Regulation	Responsible Authority	Additional Information
Suspicious Transaction Reports (STR) [Required Disclosure]	Sections 94 and 95	CTD of the FID	
Protected and Authorised Disclosures	Section 100	CTD of the FID	
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 an "Authorised Officer".
AML Guidance and implementation of AML measures and monitoring compliance with the AML laws and guidance.	Sections 91 and 91A	Competent Authority	The Betting, Gaming and Lotteries Commission for the gaming sector; The Casino Gaming
Forfeiture and Pecuniary Penalty Orders	Sections 5 (31)	ARA DPP	
Restraint Orders	Sections 32 and 33	ARA, DPP	

62. *Fixed Penalties*

Section 138 of POCA allows the Commission to issue fixed penalty notices in respect of offences for breaches of specified Regulations, if the Commission has reasons to believe that the entity has committed any such offence.

A fixed penalty notice is a notice in writing, completed on a prescribed form, offering the entity to which it is issued the opportunity to discharge any liability to conviction of an applicable offence by payment of a fixed penalty. The notice shall:

- provide the gaming entity with the particulars of the alleged offence;
- state the fixed penalty payable by the entity and the period which proceedings will not be taken against the entity (15 days or more);
- require the entity to attend court in the appropriate jurisdiction, no later than ten days after the expiration of the period specified, by way of summons, if the fixed penalty is not paid within the appropriate time.

An entity to which a fixed penalty notice is issued shall not be liable to be convicted of the applicable offence concerned, if the entity pays the fixed penalty or if the offence is a continuing offence, the entity has taken steps to discontinue the offence.

---

[12]Section 101(2), POCA
[13]Section 104(2), POCA.
[14]Section 112, POCA.
[15]Section 122(1), POCA.
[16]Section 122(3)(a), POCA.
[17]Section 122(3)(b), POCA.

Fixed penalty payments shall be made to the Collector of Taxes.

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

(a) A forfeiture order is an order by the court that, in the case of a person's conviction for any offence in proceedings before the court, any property used in or in connection with the offence concerned be forfeited to the crown. A forfeiture order can also be made where the court determines that a person convicted for an offence has a criminal lifestyle and that person has benefited from his general criminal conduct. In this case, The Proceeds of Crime Reg the forfeiture order would be made in relation to the property identified as that person's benefit from his criminal conduct.[18]

(b) A pecuniary penalty order ("PPO") is an order by the court for the person against whom the order is issued, to pay to the Crown an amount equal to the value of the benefits derived by that person from his/her criminal conduct[19] An order of this nature would usually be made in circumstances where the property representing the benefit from criminal conduct cannot be the subject of a forfeiture order, for instance, the property cannot be located.[20]

(c) A restraint order is an order by the court prohibiting any person from dealing with any realizable property held by a specified person. Realizable property means any property held by the person who is the subject of the order; or any free property held by the recipient of a tainted gift[21].

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

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

ii. The seizure and retention of any information or material found which is likely to be of substantial value, whether by itself or not, to the investigation in respect of which the search warrant has been issued.[22]

The Act states that this warrant does not confer the right to seize any information or material in respect of which production can be refused on the grounds of legal professional privilege in proceedings in the Supreme Court.[23]

(e) A disclosure order is an order by the court that requires the person on whom it is served to either produce or grant access to, information or material to an appropriate officer or answer questions at a place or time specified in the order.[24]

The Act states that this Order does not require production of or access to information that can be refused, that is, "excluded material"[25] or information or material that can be refused on the grounds of legal professional privilege 34 in proceedings in the Supreme Court.[26]

(f) An Account Monitoring Order is an order by the court to a gaming machine operator to provide the account information specified in the order to an appropriate officer for the period and at or by the time or times specified in the order. For these purposes, account information means information relating to an account held at, or a transaction conducted with, the gaming machine operator specified in the order, by the person specified in the order, whether solely or jointly with another.[27]

Under the POCA an accounting monitoring order has effect notwithstanding any restriction on the disclosure of information, however imposed (Section 126(7)). This Order remains in effect for ninety (90) days and may be extended for a further ninety (90) days.

Criminal Forfeiture Regime

64. The criminal forfeiture process is initiated after conviction when either the ARA or the DPP applies to the Supreme Court for either a forfeiture order or a pecuniary penalty order (PPO).

65. On receipt of this application, the Court will make a determination as to whether the defendant has benefitted from criminal conduct based on the following:

i. a defendant is convicted of any offences in proceedings before the Court; or

ii. a defendant is committed to the Supreme Court from the Parish Court for the making of a forfeiture order or pecuniary penalty order.

66. In establishing whether a person has benefited from criminal conduct, the Court shall:

i. determine whether the defendant has a criminal lifestyle and has benefited from his general criminal conduct[28]; or

ii. if the Court determines that the defendant does not have a criminal lifestyle, it should determine whether the defendant has benefitted from his particular criminal conduct.[29]

---

[18]Section 5, POCA.
[19]Referred to as the "Recoverable Amount"
[20]Section 2, 5(3)(b) and 5(5), POCA.
[21]Sections 2 and 33, POCA.
[22]Section 115(3), POCA.
[23]Section 117, POCA.
[24]Section 105(3), POCA.
[25]"Excluded material" per section 103 of POCA means: (a) medical records; (b) human tissue or fluid which has been taken for the purpose of diagnosis or medical treatment and which a person holds in confidence.
[26]See Section 108, POCA.
[27]Sections 126(4) and (5), POCA.
[28]General Criminal conduct refers to all the defendant's criminal conduct occurring after May 30, 2007.
[29]Particular crminal conduct means all the defendant's conduct occurring after May 30, 2007, which constitutes:
i. the offence concerned
ii. offences of which the defendant was convicted in the same proceedings as those in which he was convicted of the offence concerned; or
iii. offences which the Court will be taking into consideration in sentencing the defendant for the offence concerned.

67. Where any property was used in or in connection with the offence concerned (that is, the instrumentalities of the crime), the Court shall make an Order for that property to be forfeited to the Crown.

68. Where the Court is satisfied that a person has benefitted from criminal conduct, the Court shall identify the property that represents the defendant's benefit and:

i. make an order that the property be forfeited to the Crown; or

ii. order the defendant to pay to the Crown an amount equal to the value of his benefits (recoverable amount).

69. A person shall be deemed as having a criminal lifestyle if:

i. the person was convicted for an offence specified in the Second Schedule;

ii. the offence for which he was convicted constitutes conduct forming part of a course of criminal activity, from which the person obtains a benefit; or

iii. the offence for which he was convicted was committed over a period of at least one month and the person has benefitted from the conduct constituting the offence.

70. Statutory safe guards to the above powers of forfeiture 40 include the following:

i. In considering whether a forfeiture order should be made the Court must take into account—

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

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

Civil Forfeiture Regime

71. The POCA allows for the civil recovery 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.

Civil Recovery of property obtained through unlawful conduct[30]

72. The enforcing authority may take proceedings in the Supreme Court against any person whom it believes holds recoverable property, that is, property obtained through unlawful conduct. For the purpose of deciding whether a person obtains property through unlawful conduct, it is immaterial whether or not any money, goods or services were provided in order to put the person in a position to carry out the conduct, nor is it necessary to show the particulars of the conduct.

73. Where a civil recovery order is made, the property is vested in the ARA except for real property that is instead vested in the Crown.

74. The ARA shall not start proceedings for a recovery order unless it believes that the aggregate value of the recoverable property that will be subject to the recovery order is not less than $250,000.

75. Recoverable property may be followed into the hands obtaining it on a disposal by:

(i) the person who obtained the property through the unlawful conduct; or

(ii) a person into whose hands it may be followed.[31]

76. Where property obtained through unlawful conduct ("the original property") is or has been recoverable, any property that wholly or partly represents the original property is also recoverable property.[32]

77. Where a person enters into a transaction in which:

i. he disposes of recoverable property, whether the original property or property which represents original property; and

ii. he obtains other property in place of it, the other property represents the original property.[33]

78. If a person disposes of recoverable property, the property may be followed into the hands of the person who obtains it and continues to represent the original property.[34]

79. If a person's recoverable property is mixed with other property, whether belonging to that person or not, the portion of the mixed property that is attributable to the recoverable property represents the property obtained through unlawful conduct.[35]

---

[30]Unlawful conduct means:
(a) conduct that occurs in, and is unlawful under the criminal law of Jamaica; or
(b) conduct that occurs outside of Jamaica and is unlawful under the criminal law of that country and is also unlawful under the criminal law of Jamaica.

[31]Section 84(2), POCA.
[32]Section 85(1), POCA.
[33]Section 85(2), POCA.
[34]Section 85(3), POCA.
[35]Section 86, POCA.

80. Where a person who has recoverable property obtains profits accruing in respect of the recoverable property, the profits shall be treated as representing property obtained through unlawful conduct.[36]

Cash Transaction Limits (Section 101A POCA)

81. Section 101A, POCA has introduced a limit of J$l 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.

82. The word "transaction" refers to all currency transfers including cash-in and cash-out of a gaming machine operator.

i. "cash in" means a transaction involving the receipt of cash paid by or on behalf of a patron to a gaming machine operator, and includes:

   (a) cash received by the gaming machine operator in exchange for gaming credit to be used in the gaming devices (slot machines, electronic table games);

   (b) a deposit of cash to be credited into the patron's account with the gaming operator;

   (c) cash received by the gaming operator in settlement of any debt owed by the patron to the gaming machine operator or for the redemption of any cheque held by the gaming machine operator; and

   (d) cash inserted into a gaming machine (which is not linked to an automated system).

ii. "cash out" means a transaction involving the payout of cash by a gaming machine operator to or on behalf of a patron, and includes:

   (a) cash paid by the gaming machine operator to redeem credit;

   (b) cash paid upon a withdrawal made from the patron's account with the gaming machine operator;

   (c) cash paid by the gaming machine operator as a complimentary item;

   (d) cash paid by the gaming machine operator as winnings in any tournament, contest, or other draw or game; and

   (e) cash winnings derived from a jackpot obtained on a gaming machine (seat) or electronic table game.

iii. "Winnings" paid to a patron is, therefore, a currency transaction that falls within the ambit of the types of transactions set out in the 101A provision. Such a payment would be made to satisfy "indebtedness, accounts payable or other financial obligation" by the gaming machine operator.

83. A person shall not:

i. pay or receive cash in excess of the prescribed amount in a 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

ii. 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.

84. It therefore means that every cash transaction with a patron involving either cash in or cash out over J$l million in a single transaction or multiple cash transactions which the gaming machine operator knows are entered into by or on behalf of a patron, or the aggregate of which is either cash in or cash out over J$l million in any gaming day could constitute a breach of the section.

85. A "gaming day" is defined as a 24-hour period which constitutes a normal business day of a gaming machine operator, being the same period by which the operator keeps its books and records for business, accounting and tax purposes.

86. Gaming machine operators are required to implement steps that will allow for the monitoring of monies paid in by and monies paid out to customers. Monitoring cash-in and cash-out is a standard requirement of the Financial Action Task Force (FATF). This is expected for single transactions as well as multiples that exceed the threshold and so winnings are considered to be transactions to be monitored.

87. The following transactions may not be factored for the purposes of ascertaining whether the single transaction exceeds the J $l million:

- Cash ins, to the extent that the same physical currency was wagered previously to a money play on the same gaming device without leaving the gaming device; and
- Cash outs, where a portion of the winnings are withdrawn from a customer's account, not exceeding the cash limit, and the remaining winnings used to continue gaming.

Statutory AML Obligations under the POCA and POC (MLP) Regulations

88. Statutory AML obligations under the POCA regime can be found in Part V of the POCA and in the POC (MLP) Regulations and require the following:

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

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

iii. Complying with the directions of the Designated Authority in relation to required disclosures

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

v. Complying with other AML operational and regulatory controls under the POC (MLP) Regulations, 2007.

---

[36]Section 87, POCA.

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

89. 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.

The circumstances are as follows:

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

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

iii. 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.

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

i. 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

ii. 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.

90. With regards to the STR obligations, gaming machine operators should note:

i. 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);

ii. For persons in the regulated sector as defined by the POCA Fourth Schedule (i.e. financial institutions, financial holding companies or DNFI's), the duty to make required disclosures in relation to suspicious transactions, arises in relation to transactions engaged in the course of business in the regulated sector, which resulted in the reporting person's knowledge or belief that another person has engaged in a transaction that could constitute or be related to money laundering.

iii. For DNFI's, required disclosures are made in the manner specified by the Designated Authority.

iv. For the purpose of determining whether a required disclosure is to be made, a business in the regulated sector must identify all:

- Complex, unusual or large business transactions carried out with the business;
- 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
- 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.[37]

v. A business in the regulated sector must make a record of all transactions and matters reflected at (iv) above and these records are to be retained for a period of not less than seven years.

Protected and Authorised Disclosures

91. 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:

i. the information or other matter disclosed was obtained in the course of the reporting 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 money laundering; and

iii. the disclosure is made to an authorized officer[38] or Nominated Officer as soon as is reasonably practicable after the said information or other matter comes to the person making the disclosure.

92. 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.

93. 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 (MLP) Regulations

94. Most of the AML operational and regulatory control requirements are in the Regulations and are outlined below:

KYC/ Customer Due Diligence ('CDD') requirements:

i. *Risk Profile*

---

[37]Section 9–(4)(b), POCA.
[38]In this section, an authorized officer is an officer of the FID, a constable or a customs officer.

95. Gaming machine operators are required to establish a risk profile for all business relationships and one-off transactions[39]. The basis on which such profiles are established should be guided by the respective risk assessments[40] undertaken by regulated entities. High-risk relationships or transactions as prescribed under Regulation 7A include the following:

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

ii. *Reasonable Due Diligence*

96. Gaming machine operators are mandated by Regulation 7A(3)[41] 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—

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

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

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

iii. *Additional KYC/CDD Requirements*

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

1. 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[42]. Identification information includes address verification.

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

- cases where the transaction involves cash at or above the prescribed amount;
- transactions appear to be linked;
- wire transfer transactions are being conducted;
- there is doubt about the accuracy of any previously obtained evidence of identity; or
- a required disclosure (STR) is to be made;

3. KYC details must be retained for electronic funds transfers throughout the payment process and chain. The KYC details must include for all the persons involved in the transaction:

- Name;
- Address;
- Account number (where applicable);
- National identification number, the customer identification number or
- the date and place of birth of the person who places the order for the transfer and the holder of the account, that is, the source from which the funds are transferred, and every recipient of the funds transferred[43]. (Regulation 9(2A)).

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)).

100. 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 (MLP) Regulations)[44].

---

[39]Regulation 7A, POC (MLP) Regulations.
[40]See PART 4 of the Guidelines.
[41]POC (MLP) Regulations (Amendment), 2013.
[42]Regulation 7(1)(c) and (d), POC (MLP) Regulations; Regulation 19, POC (MLP) Regulations.
[43]Applicable to transfers that exceed US$1,000.
[44]POC (MLP) Regulations, regulation 11 and 13—First Schedule to the POC (Amendment) Act, 2013.

101. Gaming machine operators must ensure the retention of identification and transaction records. Such records should be retained for a period of seven (7) years or for such other period as may be specified by the designated authority (Regulation 14, POC (MLP)Regulations);

102. Gaming machine operators are prohibited from maintaining anonymous, fictitious or numbered accounts (Regulation 16, POC (MLP) Regulations);

103. Gaming machine operators must ensure that the CDD update requirements are applied to existing customers. Gaming machine operators are not required to obtain information or evidence in respect of any transaction conducted prior to the relevant date, which is March 29, 2007 (Regulation 19, POC (MLP) Regulations);

104. Gaming machine operators 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.

Terrorism Prevention Act, 2005 ("TPA")

The TPA was passed in 2005, and was amended in 2010, 2011, 2013 and 2019. The TPA applies to all persons covered by section 15 (c) of the Act, who are in the regulated sector, and includes the obligations to report suspected terrorism financing activities[7].

105. The Act outlines the following offences:

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

i. intending that they be used, or knowing that they will be used in whole or in part for the purpose of facilitating or carrying out terrorist activity or for the benefit of any entity known to be committing or facilitating any terrorist activity;

ii. knowing, in whole or in part, they will be used by or will benefit a terrorist group.[45]

(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.[46]

(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.[47]

106. 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.

107. 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[48]

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;

v. 'terrorism offence' and 'terrorist activity' to include conspiracies, or attempting to commit, aiding, abetting, procuring or counselling activities.

'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.

---

[45]Section 4 of the TPA.
[46]Section 5 of the TPA.
[47]Section 6 of the TPA.
[48]TPA Sections 2(2) and 2(7).

108. The TPA also requires that gaming machine operators:

(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[49] 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[50] [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;

ii. or 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.[51]

(b) Report all suspicious transactions to the Designated Authority [Suspicious Transaction Report][52].

(c) 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[53].

(d) 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.

(e) Gaming machine operators must designate a Nominated Officer at management level who should arrange for independent audits to ensure that compliance programmes are effectively implemented[54].

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
Duty of entities to file a Listed Entity Report	Sec. 15	FID
Duty to file complex or unusual large transactions	Sec. l6(3)	FID
Duty to file STRs	Sec. 16(3A)	FID
Tipping off	Sec. 17	FID
Implementation of regulatory controls to prevent TF	Sec. 18	Competent Authority
Account Monitoring Orders	Sec. 19 and 20	Relevant Authority 55
Examination and Production Orders	Sec. 21	Relevant Authority
Search Warrant	Sec. 23–27	A Constable named in the Warrant
Forfeiture Orders	Sees. 28–33	Relevant Authority
Restraint Orders	Sees. 34–43	Relevant Authority
Disposal (i.e. resolution of) property seized, restrained, etc.	Sec.44	Relevant Authority

109. 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).

110. The foregoing orders operate with similar effect to those described under the POCA, except for the following differences:

(a) *Account Monitoring Orders*

Account information is not defined, but, as is the case with the POCA, the monitoring order is applicable to information regarding transactions conducted through an account by a particular person with the institution. There is no express wording that reflects the order takes effect regardless of any restriction on the disclosure of the information however imposed, as is the case under the POCA at section 126(7).

---

[49]The Terrorism Prevention (Amendment) Act, 2013, new section IS(l) and new subsection (9). In March 2006 the Mnister designated the CTD of the FID the Designated Authority for the purposes of reporting obligations and other specific obligations outlined at sections 15–18 of the TPA. Section 15 TPA has been amended to indicate that the ctd of the FID is the Designated Authority.
[50]Section 15, TPA.
[51]Section 14, TPA.
[52]Section 16, TPA.
[53]Section 18, TPA.
[54]Section 18 of the TPA.
.

(b) *Examination and Production Orders (sections 2.1 and 22)*

The Relevant Authority can apply to the court for information or documents to be made available for an examination or for a production order. The application is made *ex parte* in writing and accompanied by an affidavit, and if granted, the subject entity would be directed by the judge to make the information or documents available for examination by a Constable named in the order, or to produce the information or documents to the Constable.

(c) *Statutory safeguards to the powers of forfeiture (section 28(5))*

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

i. In considering whether a forfeiture order should be made, the Court must take into account:

- Third party rights and interests in the property;
- The gravity of the offence concerned;
- Any hardship that might reasonably be expected to be caused by the order;
- The use that is ordinarily made of the property or the intended use of the property.

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

iii. Persons claiming an interest in the property targeted for forfeiture may apply to the court for an order and the Court, if it is so satisfied shall make an order declaring the nature, extent and value of the person's interest in the property. Before such an order is made, the court must first be satisfied that the applicant was not in any way involved in the commission of the offence; that the person acquired his interest for sufficient consideration and without knowing or having reasonable grounds to suspect that at the time the property was acquired, it was used in, or derived from, obtained or realized directly or indirectly from, the commission of a terrorist offence (section 31(2)).

The Terrorism Prevention (Reporting Entities) Regulations

111. The Terrorism Prevention (Reporting Entities) Regulations were promulgated in March 2010. These Regulations outline the operational procedures that must be maintained by gaming machine operators particularly for the commencement of a business relationship or conducting a one-off transaction. These regulations largely mirror the POC (MLP) Regulations and require gaming machine operators to establish and maintain appropriate procedures in relation to establishing a risk profile for all business relationships and one-off transactions, identification of customers (including identification of the ultimate beneficial owner or person who ultimately controls a legal person), record-keeping (minimum 7 year retention period), internal controls, communication, and training of employees. These Regulations also prescribe the reporting requirements for transactions, which the reporting entity knows, or suspects may constitute a terrorism offence (Suspicious Transaction Report); and a report every four months as to whether or not the reporting entity is holding property etc. in respect of a listed entity (Listed Entity Report).

112. Under the Counter Financing of Terrorism (CFT) framework, an institution is required to report whether:

(a) the institution is in possession of property for a listed entity (section 15); or

(b) the institution is in possession of property for a person included on the UN consolidatedlisting of individuals and entities pertaining to AI-Qaida pursuant to United Nations Counter-Terrorism Security Council Resolution 1267 (1999)—Afghanistan (section 15); or

(c) The institution is of the view that a transaction constitutes a transaction described at section 16 of the TPA (i.e. suspicious, unusual, complex etc.,[56] involving property connected with or intended to be used in the commission of a terrorism offence etc.[57]

The requisite report must be made to the Designated Authority using either Form 1 [a report in relation to (a) or (b)], or Form 2 [a report in relation to (c)].

The United Nations Security Council Resolutions Implementation Act (UNSCRIA)

113. The United Nations Security Council Resolution Implementation Act was passed in November 2013, amended November 2019 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 (40) Recommendations, 2012.

114. This Act is an enabling legislation that forms the basis for Jamaica to respond to directives or resolutions issued by the UNSC by promulgation of the requisite Regulations under this Act. Accordingly, the Act defines certain terminology (section 2):

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

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

---

[55]The Relevant Authority is either the DPP or the FID
[56]The (Terrorism Prevention (Amendment) Act, 2011 section 16(3).
[57]The Terrorism Prevention (Amendment) Act, 2011 section 16(3A).

(c) "financial institution";

(d) "relevant authority" (that is, regulator of financial institutions or financial services -such as the BOJ and the FSC), regulator of designated non-financial institutions (such as the Public Accountancy Board, the General Legal Council, the Real Estate Board, the Betting Gaming and Lotteries Commission and the Betting Gaming Commission); border control authorities (such as Jamaica Customs Agency and PICA),[58]defence authorities (such as the Coast Guard and the JDF), entity with responsibility for foreign relations (i.e. MFAFT),[59]the Jamaica Constabulary Force; any other entity to whom a UN sanction enforcement law requires information or a document to be given;

115. The Act provides for the following:

(a) Imposes a duty on financial institutions and DNFIs 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[60]. These reports are to be made to the designated authority, which is defined in the Act, to be the CTD of the FID[61]. Reporting in this regard must be done in compliance with any directions that may be given by the Designated Authority, (section 5(4)); and the fact that a report has been made must not be disclosed to any other person, (section 5(6)). These reports are due once every four calendar months. Reports are also due upon request of the Designated Authority[62].

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

(d) Provides for monitoring compliance with any UN sanction enforcement law by empowering the regulated authority by written notice to request from any person the information or documents specified in the notice. Non-compliance with this request constitutes an offence (sections 14 and 15) however a person is not required to give any information or document in response to a request, if to do so would violate legal professional privilege.[63]

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

116. 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 Regulation under this Act giving effect to such a decision and outlining the specific parameters of compliance (section 3). One set of Regulations in this regard was issued simultaneously with the passage of this Act in relation to the jurisdiction of the Democratic People's Republic of Korea.

117. The UNSCRIA also prohibits any person in Jamaica and any Jamaican outside Jamaica from knowingly—

(a) dealing directly or indirectly with any assets that are owned or controlled by or on behalf of, or at the direction of, the person or entity that is proscribed, including funds derived or generated from property 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 other related service 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[64].

The United Nations Security Council Resolutions Implementation (Asset Freeze—Democratic People's Republic of Korea) Regulations

118. The UNSC Resolutions Implementation (Asset Freeze - Democratic People's Republic of Korea) Regulations, 2013[65] 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 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.

119. These Regulations criminalize the following activities:

(a) holding, using or dealing with freezable assets owned or controlled by a designated entity; and

(b) making an asset available to a designated entity, otherwise than, in accordance with the Regulations[66].

---

[58]Passport, Immigration and Citizenship Agency.
[59]Ministry of Foreign Affairs and Foreign Trade.
[60]Section 5, UN Act.
[61]Section 5(1), UN Act.
[62]Section 5(3), UN Act.
[63]Section 14(7), UN Act.
[64]Section 8A of the UNSCRIA.
[65]Schedule to the UNSEC Resolutions Implementation Act, 2013.
[66]Section 3 of the United Nation Security Council Resolutions Implementation (Asset Freeze—DPRK) Regulations.

A person is found in contravention of these Regulations if—

(a) the person—

i. holds a freezable asset;

ii. uses or deals with the freezable asset;

iii. allows the freezable assets to be used or dealt with; or

iv. facilitates the use of the freezable asset or dealing with the freezable asset;

(b) the use or dealing mentioned in paragraph (a) is not by virtue of permission given by a notice from the Minister, under Regulation 7[67]; and

(c) the person directly or indirectly, makes 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)).

120. 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).[68]

Areas of Enforcement under UN Act, 2013 and UNSEC Implementation (Asset Freeze-DPRK) Regulations, 2013

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	
Non-financial institutions 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	
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	
Cooperation of Government entities	Sec. 13	Relevant Authority	See paragraph 110 above for definition of 'relevant authority'
Implementation of regulatory controls to ensure compliance	Sec. 21 and Regs., under the Act	Competent Authority	Regulations not yet developed.
Contravention of a UN sanction enforcement law.	Secs.10 and 11	Relevant Authority (defined in para. 74)	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) and 11(4)	Relevant Authority	Compliance is monitored by the Relevant Authority under s.13 of the Act.

[67]Section 5 of the United Nation Security Council Resolutions Implementation (Asset Freeze—DPRK) Regulations.
[68]Section 7 of the United Nation Security Council Resolutions Implementation (Asset Freeze—DPRK) Regulations.

Areas of Enforcement under UN Act, 2013 and UNSEC Implementation (Asset Freeze-DPRK) Regulations, 2013, contd.

Areas of Enforcement	Act or Regulation	Responsible Authority	Additional Comments
Permission to use or deal with a freezable asset.	Reg. 7 DPRK	Ministry with portfolio responsibility for Foreign Affairs and Foreign Trade by	Applications would be done in relation to prohibitions contained in specific implementing Regulations issued under the Act.
Offences under the Regulations on DPRK (refer to paragraph 51 above)	Regs. 4, 5 and 6	Office of the Director of Public Prosecutions (ODPP)	

Designation of Proscribed Persons and Entities Under the UNSCRIA

121. A person or entity may be designated as proscribed by section 3 (2) of the Act or through an application made by the Director of Public Prosecution's (DPP) to a Judge of the Supreme Court for an order to affirm a person or entity as a proscribed person or proscribed entity. Upon the declaration of a person or entity as a proscribed person or proscribed entity by the Judge, via an order, the relevant authority is mandated to:

a. provide notification of all designations and de-listings of proscribed persons and entities; and

b. issue guidelines on measures to prevent proliferation financing[69].

122. The Minister and the Designated Authority shall cause a copy of the order to be published—

a. on its public website within twenty-four hours after the order is made; and

b. in a daily newspaper in circulation in the island[70].

Other Relevant Legislation

The Financial Investigations Division Act

123. 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 TP (Amendment) Act (section 15)); and The United Nations Security Council ('UNSC') Implementation Act (section 5(1)). FID statistics and publications including advisories to financial institutions and to DNFIs can be accessed from its website at www.fid.gov.jm.

124. The Designated Authority, as a supervisory authority, maintains statistical records, as it considers appropriate, for the purpose of measuring the overall effectiveness of measures taken with respect to the prevention of money laundering, terrorist financing or proliferation financing. Under this section of the Act the FID also has the power to disclose to any authorized entity listed within sections 137A (4) and 18B (4) the statistical information it has recorded, if the information does not include any information from which the identity of a person, or any personal details in respect of any person, is ascertainable either on the face of the disclosure or by reasonable inference.[71]

125. The Dangerous Drugs Act, 1948 (amended 2015) The Extradition Act, 1991 The Firearms Act, 1967 (amended in 2010) The Mutual Assistance (Criminal Matters) Act, 1995 The Sharing of Forfeited Property Act, 1999 Criminal Justice (Suppression of Criminal Organization) Act, 2014 Law Reform (Fraudulent Transaction) (Special Provisions) Act, 2013 Cyber Crimes Act, 2015 as well as other legislation relating to fraud, dishonesty, and corruption.

PART 3—INTERNATIONAL REGULATORY REQUIREMENTS

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

126. This established the following main obligations for member states of the United Nations:

a. Criminalization of participation in an organized criminal group;

b. Criminalization of the laundering of the proceeds of crime;

c. Measures to combat money laundering;

d. Criminalization of corruption;

e. Measures to address the liability of legal persons;

f. Legal framework that adequately addresses, among other things,

---

[69]Section 14A of the UNSCRIA.
[70]Section 3A of the UNSCRIA.
[71]Section 137A of the Proceeds of Crime (Amendment) Act, 2019 and Section 18B(4) of the Terrorism Prevention (Amendment) Act, 2019.

i. The prosecution and sanctioning of offences; Confiscation and seizure;

ii. International cooperation for purposes of confiscation;

iii. Extradition; and

iv. Mutual legal assistance.

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

127. This established the following main obligations for member states of the United Nations:

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

(b) Criminalization of the conversion or transfer of property knowing that the property was derived from any of the 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 (U.N.) International Convention for The Suppression Of The Financing Of Terrorism 1999

128. This established three main obligations for member states of the United Nations:

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

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

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

129. 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.

U.N. Resolution 1373 (2001)

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

131. Because of the United Nation's characterization of acts of terrorism as threats to international peace and security, the United Nations is entitled to take, if necessary, the collective measures ("sanctions") under Chapter VII of the United Nations Charter.[72] To this end the MFATF receives from time to time, an updated listing of individuals and entities which the UN has added to its consolidated list pertaining to Al-Qaida pursuant to United Nations Counter-Terrorism Security Council Resolution 1267 (1999)-Afghanistan. This listing is forwarded to the DPP for the purpose of being addressed pursuant to the listed entity regime. Licensees/registrants may, notwithstanding the foregoing, wish to apprise themselves directly from the United Nations website and in that case may take note that the complete list and updates may be regularly accessed through the United Nations website.[73]

132. Jamaican authorities are also guided by international obligations and standards such as: The (2012) revised Forty Recommendations of the FATF on the Detection and Prevention of Money Laundering and Terrorist Financing.

133. In conjunction with these Guidelines, gaming machine operators should be guided by the FATF standards, principles and recommendations in establishing policies, programmes and procedures to prevent and detect money laundering and in combating the financing of terrorist activities as well as the prevention of proliferation financing.

---

[72]Suppressing the Financing of Terrorism-A Handbook for Legislative Drafting Chapter on U.N. Security Council Resolutions on Terrorism Financing-Page 15- (Prepared by the IMF).
[73]https:scsanctions.un.org.

The FATF Recommendations set out the internationally and regionally accepted principles relating to the appropriate measures to combat money-laundering, terrorist financing and proliferation financing. The revised FATF Forty Recommendations can be accessed from both the FATF and CFATF[74] websites at www.fatf-gafi.org, and www.cfatf.org. Further guidance can also be obtained from the Best Practices issued by the FATF, which though not binding, outline very useful approaches to employ in addressing the international standards. Examples of some of the guidance issued by FATF and found on its website are listed below:

(a) Politically Exposed Persons, June 2013

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

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

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

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

134. Advisories and Publication

Public statements in relation to certain jurisdictions are issued by both FATF and CFATF and are updated periodically. These public statements can be accessed from the FATF and CFATF websites.

PART 4—RISK-BASED FRAMEWORK

135. Under the FATF Forty (40) Recommendations, 2012[75] countries are required to identify, understand and assess, the money laundering, terrorist financing or proliferation financing risks posed to the country. Based on that assessment, countries must ensure that identified risks guide their national AML/CFT/CFP policies. This national risk assessment will therefore inform the overall national AML/CFT/CFP strategy and framework for a country and the implementation of appropriate risk-based measures for the relevant sectors within the country. The revised recommendations also indicate that the resulting national risk-based approach employed by a country should not exempt financial institutions, and DNFBPs from the requirement to apply enhanced measures when higher risk scenarios have been identified.

136. The POC and TP Regulations[76] requires that businesses within the regulated sector establish a risk profile concerning its general operations with regard to its business products and services, distribution channels, the geographic environment in which it operates and the size and nature of its operations. The size and complexity of the operator's business will impact and ultimately determine the detail and complexity of the systems used to manage and mitigate the risks identified.

Risk Identification and Analysis

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

i. Customers and other counterparts;

ii. Countries or geographic areas;

iii. Products;

iv. Services;

v. Transactions;

vi. Delivery channels; and

vii. Operating environment [business (size, activities and complexities)]; sector;

viii. National and global issues.

The significance of different risk categories will vary from one gaming machine operator to another and from one branch to another.

138. A gaming machine operator's risk assessment should be informed by the country's national risk assessment (if available) or other assessments available from the national authorities and agencies in relation to any sector; as well as peer review assessments (such as mutual evaluation reports). However, the absence of a national risk assessment does not absolve a gaming machine operator from undertaking its own assessment of the risks posed to its operations.

139. For the analysis, a gaming machine operator should assess the likelihood of the entity being misused for money laundering, terrorist financing or proliferation 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 gaming machine operator 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

140. 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;

---

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

[75]FATF Recommendation 1 and Interpretive Note to Recommendation 1.

[76]Regulation 7A(1) of the POCA (MLP) (Amendment) Regulation, 2019 and Regulaltion 6A(1) of the Terrorism Prevention (Reporting Entities) (Amendment) Regulations, 2019.

(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/PF;

(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

141. For its risk assessment, the gaming machine operator should determine if a particular type of customer carries an increased level of ML/TF/PF risk. Based on its own criteria, a gaming machine operator 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 beneficiary;

c. Customers that use nominees, trusts, family members, third parties etc.

d. Customers whose occupation include cash intensive businesses such as gas stations, supermarkets, wholesales, market vendors etc. or running charities and other non-profit organizations;

e. Indirect relationships through intermediaries who are unregulated;

f. Politically Exposed Persons (PEPs);

g. Occasional customers that have transactions above a certain threshold.

Delivery Channels

142. The delivery channels should be included in any assessment of customer risk.

The extent to which the gaming machine operator has a direct relationship with customers, or through intermediaries or correspondent relationships, or establishes business relationships without customers being physically present are important factors in developing the risk assessment.

Transaction, Product and Service Risk

143. A comprehensive ML/TF/PF risk assessment must take into consideration the potential risks from the transactions, products and services that the gaming machine operator 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 like wire transfers, online access to accounts etc.;

c. New or innovative products or services that are not provided directly by the gaming machine operator;

d. Products that involve cash payments or receipt;

e. Non face-to-face transactions or services;

f. One-off transactions;

Risk Matrix

144. In conducting its AML/CFT/CFP risk analysis, the gaming machine operator should establish whether all identified categories of risks pose a low, moderate, or high risk to the business operations. The gaming machine operator should review certain factors, e.g. the number and scope of transactions, geographical location, business type, whether cash or wire transfer is involved etc. The combination of these factors will indicate the level of ML/TF/PF risk.

145. Gaming machine operators 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, terrorist financing or proliferation 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 organization's size and organizational structure. A risk matrix is not static and should alter as the risk factors change.

146. The gaming machine operator is to ensure that the risk identification and analysis is properly documented to demonstrate that this forms the basis of its AML/CFT/CFP policies and procedures. The BGLC will also require sight of the risk assessment and the methodology utilized.

Risk Management

147. The ML/TF/PF risk of each gaming machine operator 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/PF risk management should enable a gaming machine operator to establish a business strategy, risk appetite, adequate policies and procedures and promote high ethical and professional standards to prevent the gaming machine operator from being used for criminal activities.

148. ML/TF/PF 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 entity's organizational structure and within the structure of ML/TF/PF risk management.

Role of Management

149. 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/CFP systems.

Policies and Procedures

150. The gaming machine operator 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.

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

Review of the ML/TF/PF Risk Assessment

152. The risk assessment must be updated at least annually, or more frequently depending on the circumstances. This requires the gaming machine operator to remain up-to-date with ML/TF/PS methods and trends, international developments and 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.

When new technology is adopted, appropriate measures are taken in preparation for, and during, the adoption of such technology to assess and, if necessary, mitigate money laundering, terrorist financing or proliferation financing risks the new technology may cause.[77]

Record Keeping Requirements

153. A gaming machine operator should note that regardless of the level of risks involved, there is no exemption from record keeping requirements.

Branches and Subsidiaries/Related Companies

154. Gaming machine operators are required to advise their branches/subsidiaries (resident in Jamaica or overseas)[78] of the provisions of the Jamaican AML/CFT/CFP 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.

155. Each gaming machine operator is therefore required to assess the AML/CFT/CFP regime existing in any parish/location/jurisdiction in which its branches and/or subsidiaries/related companies operate to ensure that its respective branches and subsidiaries/related companies apply the requirements of the Jamaican law. Where the AML/CFT/CFP requirements in that jurisdiction fall short of the Jamaican requirements[79] the gaming machine operator should ensure that appropriate additional measures to manage the ML/TF/PF risks are developed, documented, implemented and communicated to the BGLC.

156. A gaming machine operator shall ensure that its local branches and subsidiaries implement, and conform to obligations under the POCA, the TPA, the UN Act and attendant regulations, as well as the Guidelines.

157. In complying with the requirement for a risk-based assessment, a gaming machine operator shall in relation to its subsidiaries and branches, ensure:

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

(b) AML/CFT internal regulatory controls (i.e. employee training; designation of a Nominated Officer; auditing of internal controls etc.) are documented (where applicable) and implemented; required disclosures (i.e. STRs) are made and any other reporting obligations are met.

(c) 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.

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

FATF Requirements for DNFI

158. The FATF Recommendations state that DNFIs should be subject to the following:

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

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

---

[77]Regulation 6(iv)(b) of the Amendments to POCA.

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

(d) Requirements for other measures such as internal controls and foreign branches and subsidiaries obligations (FATF Recommendation 18); and obligations regarding higher risk countries (FATF Recommendation 19).

Risk Based Approach for AML/CFT/CFP Supervisory Activities

159. The BGLC has adopted a risk-based approach in conducting its AML/CFT/CFP supervisory monitoring and enforcement activities. Effective supervision and enforcement are critical components of a robust anti-money laundering, counter financing of terrorism and counter financing of proliferation regime. An effective supervisory and enforcement system comprises wide ranging supervisory measures that include preventative measures and related sanctions and other remedial actions.

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

- The size of the gaming machine operator;
- The degree of ML/TF/PF risks;
- The level of compliance within the sector.

161. In assessing the effectiveness of the Commissions' AML/CFT/CFP 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 the gaming machine operations. This exclusion relies on licensing, registration or other controls (like fit and proper checks) that have been implemented;

(b) The ability to identify and maintain an understanding of the ML/TF/PF risks in the gaming entity.

(c) The ability, on a risk sensitive basis, to supervise or monitor the extent to which the gaming machine operators are complying with their AML/CFT/CFP 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 Commission is able to demonstrate that its actions have an effect on the compliance of the gaming machine operator.

162. The Commission, has developed a three-level risk profile for the gaming machine operator as follows:

Risk Profile	Rating
Low	1
Medium	2
High	3

163. The risk profile uses a combination of information from onsite inspections, responses from questionnaires, interviews, the level of high-risk customers, acceptance of cash, level of high-risk products, adverse information from the Designated Authority, law enforcement and other regulatory bodies.

164. 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

165. The BGLC's supervisory examination framework includes the following:

i. Methodologies and procedures for both off-site supervision and on-site inspections. Such reviews can either be done on its own behalf or through a third party. It shall be the responsibility of the licensee to pay the cost of all examinations whether conducted by the Commission or through a third party.

ii. Off-site monitoring tools include questionnaires on the policies, procedures, risk monitoring and reporting systems in place at the institutions.

iii. On-site assessment tools include assessing the adequacy of AML/CFT/CFP controls.

iv. Officers engaged in AML/CFT/CFP inspections are to be adequately trained and have up-to-date knowledge of AML/CFT/CFP issues.

v. In addition to supervision at individual gaming machine operator's entity, where appropriate, risk-based assessments will be conducted across all or part of the gaming sector in a thematic approach.

vi. Where feasible, efforts will be made to taking risk-sensitive measures to inspect or review.

vii. Where necessary, the BGLC will conduct follow-up and special examinations.

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

167. Other off-site monitoring tools that are being deployed by the BGLC are:

i. Thematic reviews where a particular grouping of Gaming Machine operators will be required to submit information on a particular area, for instance, customer identification measures;

ii. Meetings with the Nominated Officer and other senior staff;

iii. Interviews;

iv. Reviews of internal and external AML/CFT/CFP Audit Reports.

168. The BGLC's examination process will continue to include an assessment of the adequacy of a gaming machine operator's AML/CFT/CFP policies and systems, the licensee's compliance with these policies and systems as well as the applicable legislation and the Guidelines. Accordingly, the AML/CFT/CFP oversight of licensees by the BGLC is to:

a. assist with understanding each gaming machine operator's AML/CFT/CFP risks;

b. allow for a more targeted assessment of the adequacy and appropriateness of an entity's own risk assessments and AML/CFT/CFP policies and procedures; and

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

169. Gaming machine operators should be aware that as the Competent Authority, the BGLC can have independent interaction with the Designated Authority or an authority of equivalent jurisdiction, regarding an institution's compliance with its obligations under the applicable legislation. A gaming machine operator's breach of its obligations under the applicable legislation can, in addition to the imposition of sanctions, also be reported to the Designated Authority.

PART 5 - KNOW YOUR CUSTOMER ('KYC') AND CUSTOMER DUE DILIGENCE ('CDD')[80]

Interpretation

For the purpose of this section of the Guidelines, the terms used in this section will have the meaning set out in this paragraph:

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

"customer name" means:

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

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

"on-going measure" means, in relation to a customer or transaction, a measure that must be applied by a gaming machine operator for the duration of the business relationship or when a transaction is conducted;

"outdated 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) customer data which has 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

"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;

"records" includes records pertaining to identification, transactions, business correspondence, account files (electronic and paper), 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;

"senior officer" refers to entities regulated by the BGLC in relation to a body corporate or any other legal arrangement, means 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.

"transaction' refers to all currency transfers including cash-in and cash-out of a gaming machine operator.

(a) Currency transfer has taken place when:

- the money is paid in order to receive property or services, such as by the customer in exchange for credits or other gaming instruments; or,
- the money is paid to reduce a debt or satisfy some other financial obligation, such as payments on bets including slot jackpots (winnings) by the gaming machine operator to the customer

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

General Requirements for Know Your Customer ("KYC") and Customer Due Diligence ("CDD")[81]

170. The requirement to 'know your customer' involves satisfactorily identifying the customer and establishing details pertaining to the customer's:

i. occupation and economic activity;

ii. personal financial and business track record;

iii. source of wealth/funds;

iv. contact information;

v. 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 gaming machine operator.

171. The requirement to conduct CDD involves identifying the customer and verifying that customer's identity. 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.[82] The CDD must enable a gaming machine operator to know its customer by obtaining information on what the customer does.

172. A gaming machine operator undertaking verification, should establish to its reasonable satisfaction that the verification subject, relevant to the application for business, exists and should carry out verification in respect of the customer operating the account.

173. Gaming machine operators must ensure that as soon as practicable after contact is first made with a customer concerning the commencement of a business relationship or one-off transaction the customer produces satisfactory evidence of their identity, which must then be verified. The gaming machine operator must also apply risk management measures to the conditions under which the business relationship or one-off transaction is dealt with while verification procedures are being carried out.

174. If the institution is unable to verify the customer's identity within fourteen (14) days after the contact is first made, as required in paragraph 170, then the business relationship or one-off transaction should not proceed any further, unless permitted by the Competent Authority and the gaming machine operator should make an assessment as to whether any disclosure is required under section 94 of the POCA.

175. Gaming machine operators are prohibited from keeping anonymous accounts, fictitious names or numbered accounts. The reference to "numbered account" in POC-MLPR, Regulation 16(2) and TP-RER, Regulation 16(2), means an account that is identifiable solely by reference to the number or numbers assigned to that account.

176. In seeking to discontinue the procedures for establishing a business relationship or a transaction started or attempted; or terminate the business relationship, gaming machine operators should be mindful of the prohibition against tipping off or unauthorized disclosures outlined under sections 97 and 104 of POCA and section 17 of the TPA. Gaming machine operators should therefore be careful not to "tip off" applicants for business, customers, or any other person where a suspicion has been formed by the gaming machine operator that an offence is being attempted or has been or is being committed.

177. Gaming machine operators should ensure that they have the ability to legally terminate arrangements, transactions or the business relationship, where the gaming machine operator 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.

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

Updating KYC Records

179. Gaming machine operators should undertake regular reviews[83] of all existing customers' records (identification and other particulars) to ensure that they remain up-to-date, relevant, consistent with the gaming machine operator's risk profile of that customer and remain subject to appropriate KYC and CDD processes. These reviews should be done at least seven years from the date of the commencement of the relationship and at minimum seven (7) year increments thereafter, or, at more frequent intervals to ensure the accuracy of the information held by the institution or as warranted by the risk profile of the customer.

180. The documentation provided to establish the relationship with the gaming machine operator should be continually reviewed and updated. The contract with the customer should place an obligation on the customer to notify the gaming machine operator 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 gaming machine operator to be outdated.

181. Reviews[84] 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, during the course of the business relationship, doubt arises regarding the identity of the customer or the beneficial owner of the account;

---

[81]See POCA (MLP) Regulations, 2007 or. 7, 11, 12, 13); TP (Reporting Entities) Regulations, 2010 (r. 7, 11, 12, 13); and FATF Recommendations R. 10.
[82]FATF Recommendation 10 (CDD measures to be taken).
[83]POCA (MLP) Regulations, 2007 -r. 7(1)(c) and (d) and r. 19; TP (Reporting Entities) Regulations, 2010 (r. 5 and 21).
[84]POCA (MLP) Regulations, 2007 -r. 7(2)(b) and 7(3); and TP (Reporting Entities) Regulations, 2010 (regulations 5 and 6(2)(b)).

e. Where the gaming machine operator becomes aware at any time that it lacks sufficient information about an existing customer/or about the existing business relationship with a customer;

f. 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[85];

g. Where transactions carried out in a single operation or in several operations appear to be linked;

h. Where a transaction is carried out by means of wire transfers;

i. Where there is any doubt about the veracity or adequacy of previously obtained evidence of identity;

j. Where the gaming machine operator is required to make a report under section 94 (STR) or 95 (STR by the Nominated Officer) of the POCA, or under section 16(3) of the TPA (STR).

182. If, during the course of the updating exercise or any time after the business relationship has commenced, the gaming machine operator discovers that the information on file is inaccurate, or is no longer applicable, and the correct or updated information is not available or is, in the view of the gaming machine operator, unreasonably withheld, then the gaming machine operator must take steps to terminate the relationship[86] and should consider referring the matter to the Designated Authority. The records of the conduct and results of this exercise should be in writing and available on request, to the Competent Authority, and the Designated Authority within the time indicated in the request,[87] and should also be available to the auditors (internal and external) where applicable, of that institution. In such cases, those accounts should be legally terminated unless a direction/ request to the contrary is received from the Designated Authority.

183. Where there are gaps in the KYC database[88]gaming machine operators 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/CFP 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 name as defined in the Guidelines, then the information on the gaming machine operator'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. Gaming machine operators should ensure that the records reflect the current information;

(d) correcting errors or addressing inaccuracies.

184. The KYC processes should be implemented in a manner designed to minimize the disruption of business. Customers in this category may be provided with advance notification of the information required and given a reasonable timeframe within which to comply.

Identification of Natural Persons

185. Identification must be obtained from documents issued by reputable sources that 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 issued by the authorities in the country in which the person is resident;

(c) valid voter's identification card;

186. The following information is required to satisfy basic KYC requirements for natural persons and any customer information order served on the gaming machine operator[89]:—

(a) Customer Identification Information;

(b) Customer Account number and transaction number;

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

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

(e) Transaction date and description of transaction type (e.g. deposit/cash-in, winnings);

(f) Source of funds that will be used in the transaction or used to access the service offered by the gaming machine operator;

(g) Source of wealth;

(h) Occupation or economic activity generating the source of income;

---

[85]POCA speaks to the following prescribed amounts • a TTR limit for cash transactions (see regulation 3 of the POC (MLP) Regulations (not applicable to gaming machine operators) and cash transaction limits (see POCA section 101A). No amounts are prescribed under the TPA or regulations thereunder.

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

[87]Regulation 14(4) of the POC Regulations amended 2013 (NB. Regulation 14 of the TP (Reporting Entities). These regulation speak to the record keeping obligation of reporting entities).

[88]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) is required (regulation 19-POC (MLP) Regulations amended 2013.

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

(i) Business and personal contact details;

(j) 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)

187. The following information[90] must be obtained from all prospective customers:

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

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

(c) Date and place of birth;

(d) Nationality;

(e) Taxpayer Registration Number (TRN) or other reference number;

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

188. Under the POCA (MLP) Regulations, customer information includes the TRN or other reference number. The BGLC 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

189. The permanent address of the applicant for business should be verified by an independent and reliable source. The following methods may be used[91]

a) Recent bill from a utility provider such as a telephone, internet, cable, water or electricity service provider;

b) Telephone Directory;

c) Voter Identification Card;

d) Driver's Licence.

Verification of CDD. KYC and Transaction Details

190. The name, permanent address and employment/business details of a customer should be verified by an independent and reliable source, and validated as follows:

(a) Requesting a utility bill in the name of customer with its date not past three (3) months, for example, electricity, telephone, water, cable and internet;

(b) Checking a local telephone directory;

(c) Checking with the Electoral Office of Jamaica;

(d) Driver's Licence which should be confirmed with Tax Administration Jamaica (TAJ).

(e) Passports which should be confirmed with the Passport, Immigration and Citizen Agency ('PICA').

191. Verification is a cumulative process, except for small one-off transactions, 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" is likely to mean 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

192. Gaming machine operators 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 in paragraph 184 above;

(b) 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);

(c) 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);

(d) Tax Compliance Certificate (TCC)[92] or other equivalent official confirmation from the relevant tax authorities of compliance with income tax obligations;

---

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

[91]See methods of validating of documents used for verification purposes.

[92]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.

Customers Resident Overseas

193. Gaming machine operators occasionally open accounts or form business relationships with persons who reside overseas. Gaming machine operators should apply equally effective customer identification procedures and on-going monitoring standards to non-resident customers as for those available for personal interview. Based on the inherent risks for these accounts, additional factors must be included in the due diligence and broader KYC processes and measures that are applied.

194. 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, gaming machine operators should have specific and adequate measures to mitigate the higher risk.

195. These measures to mitigate risk may include:

(a) certification of documents presented;

(b) requisition of additional documents; and

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

196. Gaming machine operators are required to ensure that, among other things, a gaming machine operator's AML/CFT/CFP 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.[93] For the purposes of these Guidelines, the jurisdictions targeted for this special attention include jurisdictions flagged by:—

(a) FATF;

(b) One or more of the other eight (8) FATF Styled Regional Bodies ("FSRB");

(c) UNSC, and

(d) 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.

Natural Persons Resident Overseas

197. The identification and KYC requirements for natural persons resident in Jamaica also apply to natural persons resident outside of Jamaica. Gaming machine operators are required to obtain the same identification documentation or their equivalent for prospective customers' resident outside of Jamaica.[94]

Verification of Identification Details Post-Commencement of Business

198. POCA (MLP) Regulation 7 speaks to situations in which satisfactory evidence of a customer's identification can be obtained as soon as is reasonably practicable after contact is first made between that person and an applicant for business. Before proceeding, a gaming machine operator must be in a position to provide documentary evidence of the evaluation it undertook to satisfy itself that it could proceed with the transaction. This includes evidence of considerations that at a minimum should include—

(a) The nature of the proposed business relationship;

(b) The nature of the transaction(s) contemplated;

(c) The geographical location of the parties;

(d) Practicality of proceeding, i.e. entering into commitments, or facilitating transactions before confirmation of the identification is obtained, (included in this consideration is whether proceeding is essential to not interrupting the normal conduct of business);

(e) Assessment of the risks to the institution, if it proceeds without confirmation of the customer's identification.

Transaction Verification

199. Transaction verification involves ensuring that the transaction indicated and conducted is the one intended by the customer/counterparty. Verification processes therefore contemplated by the Guidelines include—

(a) Ensuring that the customers have tendered evidence of the requisite 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 transactional/information flow from gaming devices, source of wealth, source of funds etc.

(c) Consistency of transaction being conducted with transaction patterns for the account history.

200. The 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 customer, should be flagged.

201. Under the POC (MLP) Regulations, a record of each transaction conducted must be kept in a manner that will facilitate the reconstruction of such transactions.[95] A gaming machine operator should also ensure that evidence of transaction verification it has undertaken 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. This information should also be readily available to the auditors of the gaming machine operator.

---

[93]POCA (Amendment) Act, 2013 section 94(A).
[94]POC (MLP) Regulations and the TP (Reporting Entities) Regulations include in the description of 'high risk' customers, a person who is not ordinarily resident in Jamaica.
[95]POC (MLP) Regulation 14(4).

Simplified and Enhanced Identification and KYC Requirements

202. The FATF Recommendations allow for either enhanced measures or simplified measures to be applied to specifically defined customers and products that have been assessed as presenting a higher risk or lower risk of ML/TF.[96]Where higher risks for ML or TF are identified by a country, it should prescribe either that financial institutions and DNFBPs take enhanced measures to manage and mitigate these higher risks and ensure that such information is taken into account when undertaking their respective risk assessments.[97]

Simplified Measures

203. Where a gaming machine operator has determined that a business relationship or one-off transaction is low risk the gaming machine operator may, with the written approval of the Competent Authority, apply simplified due diligence procedures[98].

204. In assessing whether there is a low degree of risk, gaming machine operators must bear in mind that the presence of one or more risk factors may not always indicate that there is a low risk of money laundering and terrorism or proliferation financing in a particular situation.

205. Prior to the application of Simplified Due Diligence measures gaming machine operators must meet the requirements set out in paragraph 206 and obtain written approval from the Competent Authority.

206. Gaming machine operators must meet the requirements below by[99]:

(a) Conducting an assessment as discussed in PART 4 of the Guidelines which justifies the adoption of the simplified due diligence procedure; ensuring the assessment is reflective of the country's assessment of its ML/TF/PF risks;

(b) Documenting the assessment methodology (including data source; active periods covered by the assessment; basis for methodology and findings);

(c) Implementing appropriate controls and systems to reduce or mitigate ML/TF/PF risks which should be documented and readily available to the Supervisor/Competent Authority, Designated Authority and/or external auditors);

(d) Implementing appropriate controls and systems to ensure the assessment is kept up-to date (i.e. assessments being undertaken frequently where warranted) and employing enhanced due diligence procedures should there be any change in circumstances which renders the business relationship or one-off transaction high risk;

(e) Demonstrate satisfactory level of compliance with the Act, Regulations made under the Act and all other laws concerning ML/TF/PF; and

(f) With the agreement of the Designated Authority, the matter is an appropriate one for the application of simplified due diligence procedures.

207. Written approval for the application of simplified due diligence will not be granted by the Competent Authority unless it is satisfied with the requirements in paragraph 206.

208. Where a gaming machine operator is unable to apply the required simplified due diligence measures within fourteen (14) days after contact is first made:

(a) the business relationship or one-off transaction shall not proceed any further, unless conducted with the permission of, and in accordance with guidelines issued by, the Competent Authority; and

(b) the gaming lounge operator shall make an assessment as to whether any disclosure is required under section 94 of the Act (disclosure as to transactions that constitute or are related to money laundering).[100]

209. Once approved, simplified due diligence procedures include any one or more of the following:

(a) requiring only one form of Government-issued identification from the applicant for business concerned, or accepting forms of identification other than Government-issued identification;

(b) accepting identification verification from third parties who are under analogous obligations with respect to customer identification and transaction verification procedures as concerns the prevention of money laundering;

(c) collecting only basic identification information, such as names, addresses and dates of birth or, in the case of bodies corporate, dates and places of incorporation;

(d) reliance on publicly available documents or such other documents as the Competent Authority may specify; or

(e) such other procedures as the Competent Authority may specify.[101]

210. Simplified due diligence will not be permitted if:

(a) A proper evaluation of the risk has not been conducted by the gaming machine operator, which justifies the adoption of the simplified due diligence procedures;

(b) There is a suspicion of money laundering, terrorism financing or proliferation financing;

(c) Gaming machine operators have determined that the business relationship or transaction poses high risk;

(d) Appropriate controls and systems have not been implemented to reduce or mitigate identified risks.

---

[96]FATF Guidance Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion, February 2013—Paragraph 68.
[97]Revised FATF Recommendations—Paragraph A4—Interpretive Note to R1.
[98]POC (MLP) Regulation 7 Section (5A).
[99]Regulation 5B of the Proceeds of Crime (Money Laundering Prevention) (Amendment) Regulations, 2019 and 6A (5B) of the Terrorism Prevention (Reporting Entities) (Amendment) Regulations, 2019.
[100]POC(MLP) Regulation 7B (Amendment) Regulations, 2019.
[101]Regulation 5C of the Proceeds of Crime (Money Laundering Prevention) (Amendment) Regulations, 2019 and 6A (5D) of the Terrorism Prevention (Reporting Entities) (Amendment) Regulations, 2019.

211. A gaming machine operator must discontinue applying simplified due diligence measures, if:

(a) it doubts the veracity or accuracy of any documents or information previously obtained for the purposes of identification or verification;

(b) its money laundering, terrorism financing or proliferation financing risk assessment changes and it no longer considers that there is a low degree of risk of money laundering, terrorism financing or proliferation financing; or

(c) it suspects money laundering, terrorism financing or proliferation financing.

212. The Supervisor/Competent Authority will review the ML/TF/PF risk profiles and risk assessments that have been prepared by the gaming machine operator to monitor whether its operations are consistent with the risk assessments and risk profiles that it has generated.

Enhanced Requirements

213. 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 by virtue of the positions held or functions undertaken by the customer or transacting counterparty.

214. Risks also increase if the customer 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 regulatory or AML/CFT/CFP framework. Risks also increase if the customer resides in, or operates from, a jurisdiction to a regulatory or supervisory framework that is incompatible with the supervisory or regulatory framework in Jamaica. Incompatibility would be measured by the absence or presence of any one or more of the following circumstances:

(a) The gaming activity in their jurisdiction is not subject to any regulation or supervision, or is not subject to an equivalent regulatory or supervisory framework; and

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

215. Under POC (MLP) Regulations and TP (Reporting Entities) Regulations, relationships or transactions that are identified as high-risk include:

(a) Politically Exposed Persons (PEPs),

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

(c) A person acting as a trustee for another in relation to the business relationship or one-off transaction concerned;

(d) Such other class or category of persons specified by the supervisory authority by notice published in the Gazette.

216. The list of relationships or transactions reflected in the regulations is not exhaustive and can be expanded by the supervisory authority under the POCA, by notice published in the Gazette. As such, gaming machine operators are subject to the statutory mandate to establish a risk profile regarding all respective business relationships and one-off transactions.[102] The law defines "risk profile" as a formal assessment made by the regulated business concerned as to the level of ML/TF/PF risk posed to the regulated business by the business relationship or transaction concerned.

217. Additional circumstances which, based on the foregoing, appear to increase the risks to a gaming machine operator doing business include:

(a) Verification of identification post commencement of the business relationship;

(b) Customers using cash-only transactions

(c) High Net Worth customers

(d) Non-face-to-face customers;

(e) Transactions by emerging technology;

(f) Customers from countries with inadequate frameworks with respect to AML/CFT/CPF;

(g) Transactions undertaken for occasional customers; or

(h) Wire transfers and other electronic funds transfers.

218. Regulation 7A(4) of the POC-MLPR and Regulation 6A(4) of the TP (Reporting Entities) Regulations 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) Examining the background and purpose of the business relationship and transactions, as far as reasonably possible;

(c) Increasing the degree and nature of monitoring throughout the course of the business relationship or one-off transaction to determine whether the transaction or the relationship appear to be suspicious;

(d) Ensuring that the findings of the examination conducted on the background and purpose of the business relationship and transactions are documented and made available, upon request, to the Designated Authority or the Competent Authority, as the case may require; and

---

[102]The POC (MLP) Regulations amended 2013—regulation 7A; The TP (Reporting Entities) Regulations amended 2013—regulation 6A.

(e) Limiting those business relationships and one-off transactions that appear or have been deemed to be suspicious, in accordance with the appropriate enhanced measures;

(f) Depending on the requirements of the case, may also include, among other things:

i. seeking additional independent, reliable sources to verify information provided or made available to the gaming machine operator;

ii. taking additional measures to better understand the background and financial situation of the customer;

iii. taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship;

(g) Increasing the monitoring of the business relationship, including greater scrutiny of the transactions;

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

High Risk Customers

A. *Politically Exposed Persons (PEPs)*

219. PEPs are individuals who have been entrusted with prominent public functions and have been deemed high risk. This category of persons includes the following persons and their relatives[103] and close associates[104]:

i. A head of state or of government;

ii. A member of any house of parliament;

iii. A minister of government;

iv. A member of the judiciary;

v. A military official above the rank of Captain;

vi. A member of the police force of or above the rank of Assistant Commissioner;

vii. A Permanent Secretary, Chief Technical Director or Chief Officer in charge of the operations of a Ministry, department of Government, Executive Agency or Statutory Body;

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

ix. An Official of any political party; or

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

220. In respect of any business relationship or transaction with any customer resident or domiciled or, in the case of a body corporate, incorporated, in a specified territory in accordance with section 94A of the Proceeds of Crime (Amendment) Act, the Competent Authority may direct that businesses in the regulated sector:

(a) impose such limits, on those business relationships or transactions, as may be specified in writing by the Competent Authority for that purpose (whether in the form of limits based on threshold amounts, prohibitions as to transactions with specified persons, or otherwise);

(b) provide any reports required at more frequent intervals, as specified in the directions;

(c) carry out, or permit to be carried out, such additional audit requirements as may be specified in the directions; and

(d) not rely on any assurance referred to in Regulation 12 of the POC (MLP) Regulation for the purposes of verifying the identity of the person or applicant or business.[105]

B. *Other High-Risk Customers*

221. Other High-Risk Customers include:

i. A person who is not ordinarily resident in Jamaica;

ii. A person acting as a trustee for another in relation to the business relationship or one-off transaction concerned;

iii. A member of such other class or category of persons as the Supervisory Authority may specify by notice published in the gazette.

iv. A business relationship or transaction with a customer that resides or is domiciled in a specified territory[106] or a country that has been identified as high-risk.

Additional Considerations

222. Given the risk assessment profile requirements under the AML/CFT/CFP regulations, as well as the risk based approach contemplated by the FATF Recommendations, a gaming machine operator would not be precluded from extending the enhanced or heightened measures to persons who are not expressly reflected in the list at regulation 7 A(6) of the POC (MLP) Regulations and at regulation 6A(6) of the TP (Reporting Entities) Regulations. 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 gaming machine operator's own risk

---

[103]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 POCA Amendment Act, 2013 Regulation 7A (7).

[104]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 POCA Amendment Act, 2013 Regulation 7A (7).

[105]Regulation 7B of the Proceeds of Crime (Money Laundering Prevention) (Amendment) Regulations, 2019.

[106]Section 94A of the Proceeds of Crime (Amendment) Act, 2019.

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 give the individual the authority to make decisions or issue directives regarding the use of public property; and

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

223. 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.[107]

224. A gaming machine operator 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. Senior management with ultimate responsibility for the institution's operations should ensure that the personal circumstances, income and sources of wealth of PEPs are known and verified as far as possible and should also be alert to sources of legitimate third-party information.

225. To mitigate the significant legal and reputational risk that gaming machine operators 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 gaming machine operator to ascertain whether a customer is a PEP and to identify persons and companies/business concerns clearly related to or connected with the PEP. The gaming machine operator should also access publicly available information to assist in the determination and confirmation of whether or not an individual is a PEP;

(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.

226. Following the commencement of business relationships, there shall be:

(a) Regular reviews of customer identification records to ensure they are kept current; and[108]

(b) On-going monitoring of PEP accounts.

227. In the exercise of enhanced due diligence, institutions shall pay particular attention to:

(a) requests from foreign persons to establish accounts with a gaming machine operator 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 whose beneficial owner is not disclosed or readily apparent;

(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, there is minimal play, funds from cash-out is shortly thereafter wired to another counterparty/customer (particularly off-shore 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 for gaming;

(g) enquiry by or on behalf of a PEP.

Non-Face-To-Face Customers

228. Opening of new accounts with non-face-to-face customers is not permitted.

---

[107]FATF Guidance on Politically Exposed Persons (Rl2 and 22) June 2013, "B" Time Limits of PEPs Status, paragraph 44, page 12.
[108]POCA (MLP) Regulations, 2007 r. 7(l)(c).

Transactions Undertaken for Occasional Customers[109]

229. An occasional customer (e.g. a non-account holder), falls within the definition of 'applicant for business' under the AML/CFT/CFP 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.[110] 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. [111] Where a gaming machine operator undertakes these transactions, satisfactory evidence of identity must be obtained, failing which, the transaction should be terminated. If the customer is not an account holder, that customer still remains subject to the CDD and certain KYC requirements set out above, and all documents, reference numbers and other relevant details relating to the transaction should be recorded and retained by the gaming machine operator for a minimum period of seven (7) years.[112]

Emerging Technology[113]

230. Gaming machine operators should proactively assess the various risks posed by emerging technologies in the use of new payment products and services[114], and design customer identification procedures with due regard to such risks.

(a) New payment products and services (NPPS) are described in the related FATF Guidance[115] as new and innovative payment products and services that offer an alternative to traditional financial services. NPPS 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.

(b) The providers of NPPS fall within the FATF definition of a 'financial institution,' where the activity involves money or value transfer services, or the issuing and managing a means of payment. Those providers should be subject to AML/CFT/CFP preventive measures including CDD, record keeping and reporting of suspicious transactions.[116]

231. Further considerations raised by FATF are that the provisions of NPPS:

i. Usually require a complex infrastructure involving several parties for the execution of payments. This raises a particular concern when it is not, or cannot be clearly established which of the entities involved is subject to AML/CFT/CFP obligations and which country is responsible for regulating compliance with those obligations;

ii. Sometimes involve the use of agents and reliance on unaffiliated third parties for establishing customer relationships and reloading services which can increase ML/TF/PF risks, particularly if the information collected is not shared with the entity responsible for AML/CFT/CFP requirements; and

iii. Often times involve entities from sectors such as MNOs[117] which are unfamiliar with AML/CFT/CFP controls and whose CDD could be limited in comparison to the regulated sector, and for which the chain of information could create difficulties for tracing the funds involved. For example, the chain of information for a single transaction could involve multiple entities, some of which may be located in different countries.

232. Examples of emerging new payment methods include: Prepaid cards, mobile payments, and internet-based payments (including virtual currencies). For these activities, the risks of ML/TF/PF are increased by the anonymity that can occur when these products are being purchased, registered, loaded, reloaded, or used by the customer. These risks are also increased where cash funding, loading or reloading is possible otherwise than through a bank account, for example via the internet, or where the technology permits access benefits passed on to third parties unknown to the issuer or can facilitate third party remittances. products and services with cash and nonbank payment options tend to obscure the origin of the funds. The vulnerability of these prepaid cards to effect illicit cross border transfer of funds is exacerbated due to the compact size of the cards (i.e. a number of cards loaded with high fund values, as against transporting large, bulky amounts of cash using cash couriers). The foregoing risks are recognized as being relative to the functionality of the product or service, and the implementation of AML/CFT/CFP risk mitigating measures, such as funding or purchasing limits, reload limits, cash access limits and restricting the ability for the product or service to be used outside the country of issue.

233. Using a risk based approach presumes that based on the risk assessments conducted, a gaming machine operator would not be precluded from providing relaxed measures for NPPS if the risk assessment confirms that the profile of the product or service or mechanism warrants such an approach to be taken and the appropriate risk mitigating measures are implemented. It should be noted that FATF recommends that the risks posed by NPPS should be identified, assessed and understood before institutions 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/PF risks with these the products to minimize vulnerabilities.

234. Gaming machine operators should also bear in mind that Jamaica has legislation in place treating with Cybercrimes and lotto scamming activities and should be cognisant of the obligations and offences described in these legislations as well as those in the Evidence Act and the Electronic Transaction Act.

PART 6—SPECIAL GUIDANCE REGARDING TREATMENT OF LISTED ENTITIES

235. Gaming machine operators are required to determine whether they are in possession of property for persons on the U.N. lists of terrorists or persons linked with terrorists.[118] Gaming machine operators 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.

---

[109]POC (MLP) Regulations, r.6; TP (Reporting Entities) Regulations, r.4.
[110]POC (MLP) Regulations, 2007 r.2; TP (Reporting Entities) Regulations, 2010 r.2.
[111]POC (MLP) Regulations, 2007 r.6 (l)(a); FATF (Revised) Recommendations R10(d). Note that the FATF recommendations (RIO) reflect that CDD for occasional transactions should be applied for transactions above the designated threshold of USo/Euro 15000 where there is no suspicion of ML (R10 lN1). Jamaica's requirements are therefore more stringent in this regard as no applicable threshold applies in relation to occasional transactions.
[112]POC (MLP) Regulations, r.14(5)
[113]FATF Recommendation 15
[114] Regulation 6(iv) of the Amendments to POC (MLP) Regulations
[115]FATF Guidance on Prepaid Cards, Mobile Payments and Internet-Based Payment Services, June 2013.
[116]lbid, paragraph 34.
[117]Mobile Network Operators.
[118]See section 15 of the TPA

236. Gaming machine operators should note that once a person has been designated a 'listed entity', by order of the Supreme Court in accordance with section 14 of the TPA, this designation will be published by the DPP in a daily newspaper in circulation in the Island. The BGLC by way of advisory will also inform licensees of all such listed entities.

237. A gaming machine operator 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 gaming machine operator is to comply with any directions given by the Designated Authority. This report is to be made on the prescribed form.[119]

238. In meeting this obligation of determining whether it has control or possession of property of a listed entity, a gaming machine operator is required to screen its databases against the consolidated listing of entities.[120]Screening should be done at the on boarding stage and periodically (recommended timeframe is every two weeks).

239. Gaming machine operators 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.)

(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 Authority, 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.[121]

PART 7— SPECIAL GUIDANCE - UN ACT ON THE FINANCING OF PROLIFERATION OF WMD[122]

240. Gaming machine operators must ensure due diligence programmes, policies, procedures and controls established pursuant to AML/CFT/CFP obligations[123] also incorporate measures to allow for the identification of proscribed entities, persons and jurisdictions.

241. Where, after November 15, 2013,[124] freezable assets or 'dealings' have been identified whether in the form of accounts established, funds held, transactions facilitated or otherwise, in relation to a designated jurisdiction:

(a) the requisite reporting should be done to the Designated Authority; and

(b) an application should be done to the Minister[125] either requesting that the gaming machine operator be permitted to use or deal with the freezable asset in a specified way (e.g. honouring contractual obligations to the point where termination or discontinuation of services or activities can be undertaken without penalty or without prejudicing the rights of a bona fide third party or counterparty) or to permit the asset to be made available to a designated entity.

(c) A copy of the application to the Minister should be provided to the Designated Authority and when a response to that application is received by the gaming machine operator, a copy of that response should also be provided to the Designated Authority.

242. During the period of the identification of freezable assets or dealings with freezable assets and obtaining written notification to use or deal with the assets in a specified way, a gaming machine operator could be liable to prosecution as holding, using or dealing with freezable assets, which is an offence of strict liability.[126] It is therefore imperative that a gaming machine operator employs the requisite screening to ascertain whether it is in possession or control of freezable assets as quickly as possible. Once such assets have been identified, any dealings that occur in relation to such assets should immediately be 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.

243. Gaming machine operators should note that in relation to a charge under Regulation 6 (directly or indirectly making a freezable asset available to a designated entity[127]strict liability will not be applicable in circumstances where the dealing in question has been permitted by written notice under Regulation 7.

244. Gaming machine operators 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 Regulations made under section 3(2)(a).

245. Each gaming machine operators is to report to the Designated Authority in the prescribed form, at least once in every four months[128] in the prescribed form set out in the schedule[129], 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 gaming machine operator shall comply with any directions as may be given by the Designated Authority.

---

[119]This form is accessible on the FIDs website at www.fid.gov.jm
[120]This can be accessed in an electronic format on the UN website.
[121]The POC (Amendment) Act, 2019 Section 94(A).
[122]Weapons of Mass Destruction
[123]Regulation 5 of the POC (MLP) Regulations and Section 18 of the TPA
[124]Date of Assent to the United Nations Security Council Resolutions Implementation (Asset Freeze-DPRK) Regulations, 2013
[125]Regulation 7 of the United Nations Security Council Resolutions lmplementation (Asset Freeze-DPRK) Regulations, 2013.
[126]Regulations 5(3) and 6(3), UN Regulations.
[127]Otherwise than as permitted by a notice under regulation 7
[128]Sections 5 (3) of the UNSCRIA
[129]Regulation 6 of the United Nations Security Council Resolutions Implementation (Reporting Entities) Regulations.

246. Gaming machine operators are required to report to the Designated Authority:

(a) Any transaction or attempted transaction that is believed or known to be related to a person or entity that is proscribed and any assets that are owned or controlled by or on behalf of such person or entity and are in possession or control of the entity;

(b) Any breach of any provision under the UNSCRIA by a person or entity that is proscribed;

(c) Any assets—

i. which are owned and controlled by or behalf of a person or entity that is proscribed;

ii. in possession or control of the entity; and

(d) Any other action that has been taken in relation to a person or entity that is proscribed in compliance with any directives or requirements under this Act.

All reports made under section 5 (3A) shall be disclosed to the regulators as an authorized disclosure[130].

247. Gaming machine operators 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.

248. Gaming machine operators are also required to implement systems for the identification and detection of the persons, entities and transactions related to proliferation financing and report these to the Designated Authority.

249. Where in relation to any jurisdiction identified by the UN Act, on which targeted financial sanctions 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 gaming machine operator 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 UN Act; and

(c) report the holding or dealing of the freezable asset to the Designated Authority.

250. An entity that is included on a list designated as terrorist entities by the United Nations Security Council and in whom an order is made may:

(a) Submit directly to the appropriate authority to receive de-listing requests pursuant to UNSCR 1730 or 1904 (as the case may require) or

(b) Forward to the Minister for transmission to the appropriate authority, a request for the de-listing of that entity from the list of entities designated as terrorist entities by the United Nations Security Council.

251. Where the Minister of Foreign Affairs and the Minister of National Security are satisfied, on a written recommendation from the Chief Technical Director from the FID and the DPP, as the criteria set out in the relevant United Nations Security Council Resolution in respect of an entity, the Minister responsible for foreign affairs shall make a request to the United Nations Security Council for the listing of the entity on the list of entities designated as terrorist entities by the United Nations Security Council.[131]

252. The written recommendation for the purposes of paragraph 248 shall include all the case information required under the relevant United Nations Security Council Resolution, to the extent that the information can be provided without compromising the interests of national security.

PART 8—TRANSACTION MONITORING AND REPORTING

REQUIRED DISCLOSURES— IDENTIFICATION AND REPORTING OF SUSPICIOUS TRANSACTONS

253. 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.

254. Section 94(3) of the POCA states that a required disclosure is a disclosure made to either the Nominated Officer or to the Designated Authority, of information or other matter on which the knowledge or belief is based, or which gives reasonable grounds for the knowledge or belief, that another person has engaged in a transaction that could constitute, or be related to ML. This report should be made on the FID's online reporting portal.

255. 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 with the commission of a terrorism offence or involve, or are for the benefit of, any listed entity or terrorist group. The report to the Designated Authority must be made using the prescribed form.[132]

---

[130]Section 5(3B) of the UNSCRIA

[131] Section 14B of TP (Amendment) 2019

[132]This form is available on the FID's website at www.fid.gov.jm

256. 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 officer.[133] In practice and for good order, reports of regulated businesses should be made to the Nominated Officer who will thereafter be required to make a disclosure to the Designated Authority.

257. In complying with the obligation to report suspicious transactions under the POCA and the TPA, a gaming machine operator 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 gaming machine operator;

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;

(b) make a record of these transactions and the related findings;[134]

(c) where the circumstances occur in relation to Section 16 of the TPA, 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 for the purposes of section 94(4)(b) of the POCA.

258. Where a gaming machine operator 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.[135]

259. Severe implications such as prosecution and/or reputation risk can arise when a gaming machine operator holds property or provides services to facilitate ML/TF/PF. The institution shall ensure that such accounts or transactions are subject to appropriate counter measures to safeguard the institution. Counter measures include action to:

(a) close the account;

(b) end the business relationship;

(c) terminate the transaction;

(d) scale down gaming services;

(e) refuse to undertake transactions above a certain amount;

(f) refuse to undertake new business with the customer.

260. The application of appropriate counter measures by a gaming machine operator will be indicative of it acting to protect itself and the integrity of the overall gaming industry. 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. Appropriate measures must be implemented to monitor.

261. Gaming machine operators 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.[136]

(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.

262. Gaming machine operators 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.

263. Gaming machine operators should have adequate systems to ensure the timely, ongoing detection and reporting of suspicious transactions, and holdings of property owned or controlled by a listed or designated entity.

264. 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 of the TPA respectively, includes:

i. identifying and taking notice of the types of transactions described in these sections of the law;

ii. the examination of the background and purpose of these types of transactions;

iii. the formal recording of the institution's findings; and

iv. the retention of the institution's findings for a period not less than 7 years.

---

[133]POCA section 94(3); TPA section 16(3) and 18(3).
[134]Section 94(4)(a) POCA; section 16(2) TPA.
[135]see POCA sections 93(2); 99 and 100(4) and (5)
[136]POCA Section 100(4) and (5);

265. Gaming machine operators must be in a position to make their findings in this regard available to the BGLC, upon request. These findings must also be available to the Designated Authority.

266. Gaming machine operators may be guided by section 97(2)(b) of the POCA which outlines disclosures made under certain circumstances, which would not be deemed as "tipping off": Subsection (b) specifically speaks to circumstances where the disclosure is made in carrying out a function the person has relating to the enforcement of any provision of the POCA or of any other enactment relating to criminal conduct or benefit from criminal conduct. A gaming machine operator would however be expected to exercise discretion and judgment to ensure that in-house disclosures to alternative designated compliance officers, 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.

267. There are certain categories of activities that are suspicious by their very nature and should alert a gaming machine operator as to the possibility that a customer is seeking to conduct illegal activities at the institution. Examples of such suspicious conduct and activities are outlined in Appendix II. This listing is not intended to be exhaustive, and only provides examples of the most basic ways by which money may be laundered and forms the catalyst for prompting enquiries about the source of funds and source of wealth and for applying enhanced due diligence measures. Gaming machine operators should also keep themselves abreast of the evolving typologies of ML/TF/PF.

268. Gaming machine operators 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.

269. Gaming machine operators should provide all requisite statutory information to facilitate any investigation resulting from the report, and to ensure compliance with reporting obligations.

270. A gaming machine operator is obliged to provide its reasons for determining that a particular transaction/activity is suspicious. The reasons for suspicion must:

i. be sufficiently detailed, clear and precise;

ii. set out the rationale for suspicion;

iii. indicate the particular unusual nature of the transaction;

iv. provide contrasting historical data; and

v. set out the chronology of events.

271. Gaming machine operators should establish systems that ensure all matters identified for reporting under the TPA or POCA are brought to the attention of the Nominated Officer. Each case must then be reviewed 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.

272. It is important to note that, once knowledge or suspicion of criminal spend is linked to a customer in one area of the business (for example, table games), it is good practice to monitor the customer's activity in other areas of the business (for example, gaming machine play).

273. The following must also be noted:—

(a) The POCA allows reports to be submitted in an electronic format to the Designated Authority[137]

(b) Gaming machine operators should establish a reporting and feedback regime for required disclosures:

i. 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.

ii. If the Nominated Officer decides that:

- the information substantiates a suspicion of ML/TF/PF, then this information should be disclosed within the statutory timeframe;
- there is uncertainty as to whether such information substantiates a suspicion, then it should nevertheless be reported; or
- the information does not substantiate a suspicion, then the reasons for not submitting the report to the Designated Authority must be recorded.

iii. The gaming machine operator's 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 and 99 of the POCA.

iv. At a minimum, the STR must have the following information:

- Reporting Gaming Lounge Information
- Name and telephone number for Nominated Employee (or his/her designate)
- Full name of customer

[137]POC (MLP) Reg. 17(3)

- TRN (or other national registration number) of customer
- Address of customer
- Date of birth of customer
- Identification information
- Transaction type
- Transaction date/period
- Transaction currency
- Transaction amount
- Jamaican dollar equivalent
- US dollar equivalent
- Reasons for suspicion (for STR)

Appropriate Consent Regime

274. For Gaming machine operators, "appropriate consent" occurs:

(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.[138]

(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.[139]

(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.[140]

275. 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.[141]

276. 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:

i. have a reasonable excuse for failing to make the disclosure before proceeding with the transaction;

ii. make the relevant disclosure on its own initiative; and

iii. make the said disclosure as soon as is reasonably practicable[142]

277. The Appropriate Consent regime established under the POCA is not contained within the TPA. Where the institution is uncertain whether a transaction is in breach of the provisions of POCA or the TPA, the institution should make the disclosure under POCA as this allows the appropriate consent regime to take effect.

Tipping Off Provisions:

278. A gaming machine operator is under strict obligations not to disclose to any person, the fact that it has made a required disclosure pursuant to section 94/95 or an Authorized Disclosure pursuant to section 100 of the POCA; or has made a disclosure pursuant to section 16(3) of the TPA, and must comply with all directions given to it by the relevant authorities.

279. The gaming machine operator may reveal the existence of an authorized disclosure under the following circumstances:

The circumstances of disclosure	POCA/TPA	Section
The disclosure is made pursuant to functions being carried out under the POCA or any other enactment relating to criminal conduct or benefit from criminal conduct;	POCA	97(2)(a)
The disclosure is to an attorney-at-law for the purpose of obtaining legal advice or for the purpose of the attorney-at-law giving legal advice and only where disclosures in this regard are not made with the intention of furthering a criminal purpose	POCA TPA	97(2)(b);97(3)(a) 17(2)(a);17(4)(a)
The disclosure is made to the Competent Authority	POCA	97(2)(d)
The disclosure is made to any person in connection with legal proceedings or contemplated legal proceedings	POCA	97(3)

[138]section 99(l)(a), POCA
[139]section 91(2)(b)(i) and 99)(l)(b), POCA
[140]section 91(2)(b)(ii) and 99(l)(c), POCA
[141]section 99(4), POCA
[142]sections 93(2) and 100(4) and (5), POCA

Protected Disclosures

280. The POCA has two provisions treating with the issue of protected disclosures:

(a) Section 100 (1), (2) and (3) state that a disclosure is protected if it satisfies certain conditions and does not breach any disclosure restraints however imposed. These conditions are:

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) Section 137 of POCA states that no civil or criminal proceedings for breach of confidentiality may be brought, nor any professional sanction for such breach taken, against any person, or a director or employee of an institution, who provides or transmits information requested by or submits reports to the enforcing authority under POCA. 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.

PART 9—THE NOMINATED OFFICER REGIME[143]

THE APPOINTMENT OF NOMINATED OFFICER AND REPORTING OBLIGATIONS

281. A gaming machine operator must designate an officer of the institution who performs management functions as its "Nominated Officer".[144]This Officer is responsible for ensuring the effective implementation of the established policies, programmes, procedures and controls to prevent and detect ML/TF/CFP activities in accordance with the relevant statutes, the Guidelines and the licensee's own policies and procedures.

282. Gaming machine operators must inform the Commission, in writing, of the identity of the Nominated Officer upon employment. If at any time, the Nominated Officer is terminated or reassigned to operate in another capacity, and a new Nominated Officer is appointed, the BGLC is to be notified.

283. In practice, the function of the Nominated Officer is most effective if that function is a position that:

(a) is sufficiently senior to allow for reporting to the Board, (or such other governing body) of the institution either directly (at Board meetings) or through a sub-Committee of the Board, on the institution's AML/CFT/CFP compliance;

(b) requires knowledge of the AML/CFT/CFP laws, framework, global practices and trends that can guide the institution in establishing and maintaining the requisite controls, policies and procedures in accordance with the statutory requirements and related framework;

(c) requires the ability and capacity to undertake the responsibility for on-going monitoring of the fulfilment of AML/CFT/CFP duties by the institution including sample testing of compliance, reviewing exception reports and being the contact point regarding all AML/CFT/CFP issues for internal and external authorities including supervisory authorities or the Financial Intelligence Unit/FID; and

(d) is independent of the business lines of the institution to allow for an objective assessment and monitoring and enforcement of the compliance of the institution's operations and decision making with its AML/CFT/CFP obligations under the country's framework and with the institution's own AML/CFT/CFP policies and procedures.

284. The Nominated Officer is responsible for reporting to the Designated Authority,[145] all such activities as required by the relevant statutes and the Guidelines, and should be in a position to provide advice and guidance to the staff, on the identification of suspicious transactions. 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/CFP laws and should consult with the Designated Authority accordingly.

285. An institution's policy manual should require the preparation and submission of reports by the Nominated Officer to the Board of Directors, at least quarterly or more frequently, as warranted by the risk profile of the institution. This is to ensure 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:

(a) An annual overview and evaluation of the overall effectiveness of the institution's AML/CFT/CFP framework, the effectiveness of AML/CFT/CFP measures implemented under each of the various operational areas and/or product and service types, as well as AML/CFT/CFP training exercises completed and initiatives pursued;

(b) The licensee's compliance with relevant legislation and the Guidelines in relation to the institution's AML/CFT/CFP reporting obligations, as well as the licensee's own policies and procedures;

(c) Particulars of the risk assessment and risk management activities (see PART 4) including:

i. Update on the gaming machine operator's overall relationship with the Designated Authority and general guidance received from that body;

---

[143](See Appendix I - List of Duties and Responsibilities of the Nominated Officer)
[144]See POCA (MLP) Regulations, 2007 r. 5(3); TPA section 18(3).
[145]POCA section 95; TPA section 18(3).

ii. Advice on any proposed/impending legislative/regulatory AML/CFT/CFP amendments, with an assessment of possible impact on the institution with appropriate proposal for the requisite operational changes required for continuing compliance.

Confidentiality Provisions

286. The Nominated Officer administering the ML/TF/PF reporting must ensure that this is a confidential process. This confidential treatment must be further extended in cases where investigations into ML/TF/PF or other financial crimes are in progress and the entity is subject to any investigatory order for e.g. an Account Monitoring Order.

287. The confidentiality procedures to be adhered to during investigations are established by law under sections 97 and 104 of POCA and sections 17 and 20 of the TPA. They are as follows:

(a) The gaming machine operator should have the requisite systems in place to ensure confidentiality of any investigative order served on it, except to the extent of complying with the order or acquiring the requisite legal advice from an attorney-at-law;

(b) The existence of the "Order" must only be disclosed to other officers or employees within the firm, if such disclosure is necessary to ensure that the relevant information is provided to the police. The Nominated Officer should, in most cases, be responsible for ensuring that the Order is complied with. He/she should be responsible for determining if other staff members "need to know" about the "Order" to assist with providing relevant information. Whenever possible, however, the Nominated Officer should provide the information to the named constable without consulting other employees;

(c) The Nominated Officer may also disclose the existence of the "Order" to the firm's attorney-at-law, when seeking legal advice; and Officers of the firm apprised of the "Order" must not disclose the existence of the "Order" to other employees.

PART 10—COMPLIANCE MONITORING INTERNAL COMPLIANCE PROGRAMME

288. 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.

289. The POCA and the TPA specifically require that gaming machine operators have systems in place for an independent audit, in order to ensure that the statutory requirements and the programmes itemized in the Guidelines and adopted in policy manuals, are implemented. An officer at the senior management level must have explicit and ultimate responsibility for the gaming machine operator's internal compliance programme, 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 strong 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 and targeted financial sanctions (TFS) 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/CFP programme and the internal and external audit functions. The timing of these reviews should be informed by, among other things, the institution's risk profile.

(g) An independent audit of the compliance policy conducted triennially, or whenever the Commission deems it necessary in relation to individual licensees, at the expense of the licensee, to ensure compliance with the relevant laws and regulations.

Policy and Procedural Manual

290. Each gaming machine operator shall:

(a) establish clearly defined policies and operational procedures with respect to its obligations under the AML and TFS legislative framework.

(b) ensure that AML/CFT/CFP policies and procedures are informed by the institution's assessment of its risks as discussed in PART 4.

(c) ensure that the AML/CFT/CFP policies and procedures are:

i. properly documented in the form of a manual which is readily available to staff;

ii. ensure that this manual is reviewed at least on an annual basis and make appropriate revisions and amendments to ensure its continued compliance with legislative provisions and supervisory directions;

iii. ensure that the manual and all subsequent revisions thereto are reviewed and approved by the Board.

291. A gaming machine operator shall ensure that the policies and programmes contained in its manual include the following:

(a) measures and procedures which are commensurate to the risks that have been identified from the institution's assessment of its risks;

(b) the establishment of procedures to ensure high standards of integrity for employees at all levels including senior and executive management levels;

(c) the development of a system to evaluate the personal employment history and financial history of all employees at all levels including senior and executive management levels. Gaming machine operators are expected to establish specific procedures for such evaluation at the point of hiring, and on-going evaluation would also be expected throughout the period of employment;

(d) the establishment of programmes for the training of employees on a continuing basis, and for instructing all employees as to their responsibilities in respect of the law, regulatory guidance and 'best practice' standards.[146]

(e) the establishment of comprehensive CDD policies and procedures, incorporating adequate customer acceptance policies and a multi-tiered customer identification programme that involves more extensive and rigorous due diligence to allow for adequate identification of ultimate beneficial owners; and are applied to high risk customers/accounts.

(f) institute controls that ensure that detection and reporting procedures are being followed and should include:

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 approval process.

(g) designation of an employee of the institution at the senior management level to be the Nominated Officer, responsible for ensuring the effective implementation of the policies, programmes, procedures and controls including reporting to the appropriate authorities, suspicious transactions and asset holdings re: listed entities or proscribed entities under the UNSCR;

(h) full co-operation and consultation with the relevant authorities, primarily the Designated Authority and the Competent Authority, for the purpose of carrying out the institution's obligations under law and best practice standards;

(i) procedures for analysis of clients' transactions to ascertain trends and to recognize indicators of unusual and/or suspicious activities, e.g. multiple small transactions aggregating to a specified limit in a month, or annually;

(j) arrangements for regular and timely internal and external audit reviews in order to ensure that there is adherence to the documented policy and procedures;

(k) provision for the heightened scrutiny of certain categories of customers and types of transactions when necessary, as well as the continuous review of existing practices and procedures in this area as part of the general internal/ external audit and control processes.

292. The procedures for a fully compliant internal compliance programme must include measures for:

(a) customer (including beneficial ownership) identification and verification prior to the commencement of business relationships and on an on-going basis thereafter, using reliable independent source documents, data or information;

(b) taking reasonable measures to establish the source of the customer's wealth as well as the source of funds involved in the transaction and transaction verification in respect of customer and other transactions prior to the commencement of the business relationship or transaction;

(c) documenting and maintaining records of transactions;[147]

(d) identifying and recording suspicious transactions and applicable property under the TPA or freezable assets under the UN Act and establishing clear procedures for ensuring the required reports are made in relation to these matters;

e) ensuring compliance with relevant legislation, and co-operation with enforcement authorities;

f) internal audit checks to ensure compliance with policies and procedures relating to ML/TF/PF;

g) the 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;

h) communication of group policies and procedures on the detection and prevention of ML/TF/PF activities and the monitoring of compliance by all subsidiaries/related companies and branches whether located in Jamaica or overseas.

293. A gaming machine operator shall adopt a consolidated approach to the establishment and implementation of its AML/ CFT/CFP policies and procedures, which shall cover the activities of all local and foreign branches and its subsidiaries/related companies.[148] In this regard, institutions should note the relevant sections of the Guidelines regarding the obligations for gaming machine operators, and responsibilities in respect of branches and subsidiaries.

PART 11—BOARD RESPONSIBILITY AND EMPLOYEE INTEGRITY AND AWARENESS

294. The Board of Directors of a gaming machine operator must have a clear understanding of the ML/TF/PF risks faced by the institution. This includes a good working knowledge of the operating risks faced by the institution (i.e. based on the services and products offered; customer base; strength of internal controls and hiring policies). The Board must also be actively aware of

---

[146]Section 94(6), POCA: Gaming machine operators must bear in mind the defences that can be raised by a person charged with an offence under POCA. A person can raise the defence of not knowing or suspecting that another person is engaging in money laundering and can also claim that the requisite training was not provided by the employer. The defence appears to require proof of both elements (i.e. lack of knowledge/suspicion and lack of training) in order to be successfully raised.

[147]POC (MLP) Regulations, Reg. 14(4).

[148]FATF Recommendation 18.

risks posed to the institution where it resides within a group or within a broader corporate structure as well as the broader risks posed to the institution from a national perspective. Risks from the national perspective include wider concerns:

i. performance of the economy;

ii. levels of crime and types of crimes to which gaming services are most vulnerable;

iii. the country's external ratings in the areas of credit risk, transparency, and cooperation; and

iv. inclusion in watch lists or lists which require other countries to apply certain economic measures (including financial sanctions) before or when undertaking dealings with the country.

295. The Board of a gaming machine operator must be satisfied that:

(a) the institution's risk assessment accurately and appropriately reflects the ML/TF/PF risks faced by the institution and accurately reflects the effectiveness of the measures to address these risks, and to ensure that this objective is met on an on-going basis;

(b) the Nominated Officer is appropriately qualified and has the requisite stature and authority to undertake the responsibilities of that function and to effectively execute that function (refer to PART 6). In this case, 'authority' means, sufficient scope within the institution so that issues raised by this officer receive the necessary attention from the board, senior management and business lines;

(c) the reports by the Nominated Officer are provided in a frequency that accords with the risk profile of the institution; and

(d) the institution has adequate policies and processes for screening prospective and existing staff to ensure high ethical and professional standards.

296. The Board must ensure that the institution's AML/CFT/CFP policies and procedures are effectively implemented. This means:

i. ensuring that front line, sensitive[149] and compliance functions are subject to enhanced oversight;

ii. ensuring the internal audit function assesses the risk management practices and internal controls of the institution including periodically assessing the effectiveness of the institution's compliance with its AML/CFT/CFP policies and procedures;

iii. compliance and oversight functions are provided with adequate resources to ensure that AML/CFT/CFP policies and procedures are effectively implemented; and

iv. ensuring the external audit function engagement extends to the institution's compliance with its AML/CFT/CFP policies and procedures.

297. The Board must ensure it receives adequate training on the local AML/CFT/CFP laws and framework as well as the international standards and best or sound practices which impact AML/CFT/CFP obligations for gaming machine operators.

Employee Integrity Standards

298. 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[150] of the company. Additionally, all Nominated Officers are subject to this "fit and proper" assessment.

299. 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.

300. Compliance with AML/CFT/CFP 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.

301. Supervisors and managers must know the staff in their department and report any substantial changes in their lifestyles which do not match their financial condition.

302. 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.

303. Gaming machine operators 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

304. 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.

---

[149]Sensitive functions include cash transactions, cash management functions, preparation of accounts, data input and analysis.

[150]For the purposes of paragraph 295 "officer" in relation to a company, means a person who, in that company:

a) is a key personnel in a relevant position. Key personnel include directors, shareholders, secretaries, senior officers, managers and any other position, however designated, if it is an executive position; or

b) performs functions similar to those normally performed by the holder of any position referred to in paragraph (a).

305. Gaming machine operators are required to have policies and procedures that facilitate on-going monitoring of an employee's:

i. Competence to undertake the role or position to which the employee is assigned;

ii. Compliance with statutory obligations for example, income tax and professional standard requirements;

iii. General character;

iv. Compliance with the institution's policies and procedures;

v. Adherence with ethical practices and conduct;

vi. Behaviours exhibited which accord with ethical and moral standards—behaviours in this category generally include:

- Ability to be forthright;
- Absence of or prompt declaration of conflict of interest issues;
- Absence of a culture of loophole mining (whether with internal policies or in relation to the institution's statutory obligations);
- Culture of compliance (with internal policies and with the institution's statutory obligations);
- 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 (whether or not this results in damage to the property).

306. Gaming machine operators 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; annual declaration by way of signature is required.

(b) Regular review of employee's performance and adherence to internal policies and procedures including codes of conduct and AML/CFT/CFP requirements;

(c) Imposition of appropriate disciplinary actions for breaches of the institution's AML/CFT/CFP 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[151]

307. To ensure full implementation of the procedures, recommendations, and requirements contained in the Guidelines, the staff of gaming machine operators must be made fully aware of the serious nature of AML and TFS activities. Furthermore, efforts must be made to ensure that all staff understands the basic provisions of the POCA, the POC (MLP) Regulations, the TPA, the TP (Reporting Entities) Regulations and the UN Act.

308. Members of staff must be made aware of their obligations under the POCA, the TPA and the UN Act and the fact that 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 relevant statutes.

309. Gaming machine operators must bear in mind the defences that can be raised by a person charged with any of the foregoing offences. Under the POCA, not only can a person raise the defence of not knowing or suspecting that another person is engaging in ML,but can also claim that the requisite training was not provided by the employer[152]. Under the TPA, a defence of having a reasonable excuse[153] 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.

310. 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.

311. 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.

312. Gaming machine operators 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;

---

[151]See POC-MLPR, Regulations 6, and TPA, Section 18.
[152]See POCA section 94(6)
[153] Stroud's Judicial Dictionary of Words and Phrases - discusses the meaning of the term 'reasonable excuse' with case law speaking to the meaning of the term - in a number of circumstances including ignorance of a requirement to act; honestly and reasonably believing the activity does not amount to a prohibited activity; failure to comply with a requirement on the basis of fear of self-incrimination. (8th edn. Volumes)

(b) Videotaping of scheduled training sessions. Seminar participants must be 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 gaming machine operator as a part of the audited annual report of the institution.

313. Gaming machine operators must therefore introduce training programmes to ensure that employees are informed of their responsibilities and encouraged to provide prompt notification of suspicious activities and transactions. 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/CFP 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/related companies.)

314. Training/education programmes must be designed and implemented on an ongoing basis by gaming machine operators to ensure employees' awareness of:

(a) Current as well as new and developing AML/CFT/CFP laws, regulations,

(b) Standards and guidelines being established both locally and internationally;

(c) Their legal obligations and responsibilities to detect and prevent ML/TF/PF;

(d) New ML/TF/PF techniques, methods, typologies and trends;

(e) The institution's own AML/CFT/CFP policies and procedures, including proper identification, record-keeping, internal control and communication procedures.

315. In developing education and training programmes[154], particular attention should be given to the following categories of staff:

(a) New Employees: All new employees must be informed as to the background and nature of ML/TF/PF and the need for reporting suspicious transactions/activities to the Designated Authority, through the institution's Nominated Officer. They must be informed of their personal legal obligation as well as that of the institution, to report suspicious transactions. As mentioned, institutions should also institute appropriate screening processes to thoroughly investigate the background, honesty, and integrity of prospective employees.

(b) Front Line Employees: The first point of contact of an institution with potential money launderers, persons attempting to finance terrorist activities or persons attempting to finance the proliferation of weapons of mass destruction is usually through employees who deal directly with the public. 'Front-line' staff members (such as cashiers, customer service representatives, bartenders, hostesses and receptionists) should therefore be provided with specific training on examples of suspicious transactions and how these may be identified. They must also be informed about their legal responsibilities and the institution's reporting systems and procedures to be adopted when a transaction is deemed to be suspicious. Additionally, they must be informed as to the institution's policy for dealing with occasional customers and 'one off transactions, particularly where large cash transactions are involved.

(c) Employees who deal with player account opening, or the approval of new customers must receive the same training provided to Front Line Employees. They should also be trained as to the need to verify the identity of a customer and the institution's account opening and customer verification procedures. They must further be advised that a business relationship or 'one-off transaction shall not be established or continued until the identity of the customer is verified. Employees must also be made aware that the offer of suspicious funds or the request to undertake a suspicious transaction should be reported to the Nominated Officer, whether the funds are accepted or not, or the transaction is proceeded with, or terminated.

(d) Administration/Operations Supervisors and Managers: A higher level of instruction covering all aspects of AML/CFT/CFP 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.

PART 12—RECORD KEEPING REQUIREMENTS

316. On the inception of a business relationship, the gaming machine operator is required to maintain the following records:

(a) Customer information collected during the KYC/CDD process;

(b) Customer transactions;

(c) Business correspondence with the customer;

---

[154]Interpretive Note to FATF Recommendation 18.

(d) Account Files; and

(e) Any analysis conducted on the account (including enquiries to establish purpose of a particular transaction).

317. Customer files must contain player account numbers and full customer identification information, copies of official identification documentation, account opening documentation, the results of any analysis to understand the nature and purpose of any complex and/or unusual transactions, the results of any risk assessments conducted, business correspondences and any other pertinent document.

318. Transaction records must be maintained in such a form that allows for reconstruction of each transaction and provide detailed audit trails and evidence for any criminal investigation. At a minimum, this should include the date and details of a transaction, the amounts and currencies involved and information on the conductor (customer) of the transaction.

319. Reconstruction of each transaction and the provision of information to the Designated Authority or Competent Authority upon request should be no later than seven (7) days after the request or as may otherwise be required, and to assist with tracking each customer's spending.

320. 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.

321. Retention of documents must be for seven (7) years in a form admissible under the Evidence Act. For example, where the customer closes his gaming account with the gaming machine operator or ceases to visit or use the lounge.[155]

322. 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.

323. Gaming machine operators must, in relation to each customer, make and retain for a period of not less than seven (7) years or such other period as directed by the Competent Authority in writing a record of all:

(a) complex, unusual or large business transactions carried out by that customer with the reporting entity; and

(b) unusual patterns of transactions, whether completed or not, which appear to the person to be inconsistent with the normal transactions carried out by that customer with the reporting entity.[156]

324. 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).

PART 13—APPENDICES

APPENDIX I— BASIC DUTIES AND RESPONSIBILITIES OF THE NOMINATED OFFICER

1. The Nominated Officer should be responsible for the day-to-day monitoring of the gaming machine operator'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. This duty must be independent of the internal audit function.

2. The duties and functions of the Nominated Officer should, at a minimum, include the following:

i. Act as liaison between the financial institution and the BGLC and other competent authorities with respect to compliance matters and investigations;

ii. Ensure that:

- risk assessments are carried out by the gaming machine operator;
- the appropriate risk profiles are established;
- the relevant measures and mechanisms commensurate with the risks assessed are implemented; and
- these assessments are kept up to date and relevant.

3. Evaluate new products and services (gaming devices, gaming services) to determine the risk exposure of the gaming machine operator;

4. Assist business units in the implementation of the compliance programme, including informing of regulatory changes;

5. Ensure that there are adequate systems in place for the identification of unusual and suspicious transactions;

---

[155]Regulation 14 (5)(a) of the Amendment to POCA (MLP) Regulations

[156]Section 16 (2) of the Terrorism Prevention (Amendments) Act, 2019

6. Receive and evaluate reports of suspicious/unusual transactions;

7. Ensure the timely filing of STRs, Suspicious Activity Reports (SARs) and Listed Entity Reports (LERs) to the Designated Authority;

8. Request appropriate consent from the Designed Authority;

9. Coordinate with the institution's audit, and legal departments/external legal counsel on AML matters and on TFS as notified by the UNSC;

10. Periodically provide reports to the senior management, and the board of directors on the effectiveness of the AML/CFT/CFP framework. Where applicable, this report should also speak to compliance levels with directives pertaining to TFS notified by the UNSC;

11. Prepare and update policies and procedures which should be readily accessible to the gaming machine operator's board, management, staff, and other relevant personnel and parties who may be involved in the operations;

12. Oversee administrative matters related to Code of Conduct and Compliance with AML and TFS activities;

13. Develop related training material and implement required training regime;

14. Maintain coordination between the Nominated Officers of each regulated entity within a group of companies/related companies;

15. Carry out site visits to locations/branches/units to observe implementation of internal controls procedures;

16. Utilize monitoring and audit systems to ensure compliance with all AML/CFT/CFP laws and requirements; and

17. Ensure reviews of daily transactions in order to identify unusual/potentially fraudulent activities, account excesses, *etc*.

APPENDIX II—EXAMPLES OF UNUSUAL/SUSPICIOUS TRANSACTIONS

1. The purchasing of tokens/chips, or crediting accounts, with cash and then redeeming their value by way of bank drafts, cheque or other non-cash instruments;

2. The purchasing of large value of tokens/chips with cash, playing an insignificant amount and then redeeming the value by way of non-cash instruments;

3. Use of multiple credit/debit cards to purchase tokens or add value to account/player card;

4. Use of multiple names to conduct transactions;

5. Customers whose deposits to accounts/player cards contain counterfeit notes or forged instruments;

6. Customer structures the amount spent, or value added to card so that payments fall below the threshold to avoid the Know Your Customer requirements;

7. Customer requests to add cash to winnings and then exchange the combined amount for a single cheque;

8. Customer frequently inserts substantial amounts of cash into gaming machines that have a high payout percentage and does not play 'maximum bet' to limit chances of significant loses or wins, thereby accumulating gaming credits with minimal play;

9. High volume of transaction within a short period;

10. Exchange of small denomination cash for bills of larger denomination;

11. Accumulating excessive credits on gaming machines by constantly adding cash and then cashing out to obtain large denomination bills;

12. Drastic changes in the pattern of the transactions conducted by the customer or client;

13. Customer's stated occupation or financial standing is not in keeping with their level of gaming;

14. Unemployed persons who frequently wager/gamble or add large volumes of cash to their player card;

15. An individual who was recently released from prison or is known to be involved in illegal activities is unemployed and starts to gamble large sums of money;

16. The presence of a third party for all transactions who does not participate in the actual wagering/gaming; and

17. Customers attempting to befriend employees.

18. 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. Frequent attempts to convert cash, by a customer, into a different currency from that used to initiate the transaction;

f. Cash deposits directly into gaming accounts where source of funds indicate business proceeds.

APPENDIX III—*Examples of Money Laundering Typologies in the Gaming Sector*

(a) A man convicted of dealing in drugs is released from prison and immediately starts gambling large amounts of money. He is known to be out of work and other customers inform employees that he is supplying drugs again. This will give rise to the suspicion that he is spending the proceeds of his criminal activity.

(b) Bets made by a customer become unusually high or out of the ordinary and the customer is believed to be spending beyond his or her known means. This requires some knowledge of the customer but, nevertheless, there may be circumstances that appear unusual and raise the suspicion that he is using money obtained unlawfully. It may be that the customer lives in low cost accommodation with no known source of income but nonetheless is spending money well above his or her apparent means. There is no set amount which dictates when a STR should be made and much will depend on what is known, or suspected, about the customer.

(c) Money is deposited by a customer or held over a period and withdrawn by the customer without being used for gaming. For instance, suspicions should be raised by any large amounts deposited in gaming machines or customer accounts that are then cashed or withdrawn after very little game play or gambling.

(d) A customer regularly gambles large amounts of money and appears to find a level of losses acceptable. In this instance, the customer may be spending the proceeds of crime and sees the losses as an acceptable consequence of the process of laundering those proceeds.

(e) A customer's spend increases over a period of time, thereby masking high spend and potential money laundering.

(f) A customer spends little, but often, and his annual aggregate spend is high and out of kilter with his expected spend. This could indicate potential money laundering.

(g) A customer gambles with significant amounts of money in a currency without a reasonable explanation for the source of that currency.

(h) Instances of high spend by customers that lead to significant commercial risk for the operator may also indicate suspicious activity.

APPENDIX IV—CONSEQUENCES OF NON-COMPLIANCE with POCA

Schedule of Offences under the Proceeds of Crime Act

1. All regulated entities can ensure compliance with the provisions of the AML/CFT/CFP legislation by adopting control procedures such as those outlined in the Guidelines. Indetermining whether a person has complied with the provisions of the AML legislation, (Regulations 3(3) and (4) of POC-MLPR, 2007) or the TPA legislation, (Regulation 3(l) and 3(2) of TP-RER, 2010), the court is required to take account of relevant Guidelinesand consider whether the gaming machine operator 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 institutions to consult with the Competent Authority for thepurpose of carrying out their obligations under Section 18, (Regulatory Controls by Certain Entities) of the TPA and POC-MLPR respectively.

2. Failure to comply with the provisions of the law may result in the following consequences:

Criminal Prosecution

There are penalties for breaches of the provisions of the ML/FT/FP prevention legislation, whether by firms, individuals or employees.

Commercial Losses

The institution may incur non-productive costs to address issues arising out of investigations into alleged ML/FT/FP activities, costs to defend prosecutions, and costs to repair the institution's public image.

Loss of Reputation

Institutions that, even inadvertently, become involved in ML/FT/FP activities risk loss of their good name in the market. This may occur because of media coverage of the circumstances.

SCHEDULE OF OFFENCES AND PENALTIES (POCA)

Offence	Section	Penalty- Parish Court		Penalty- Circuit Court	
		Individual	Body Corporate	Individual	Body Corporate
Failure to comply with any requirement or direction issued within the confines of the POCA by the Competent Authority.	91A(5)	N/A	Fine up to $3M	N/A	Fine
Concealing, transferring, converting, etc, criminal property.	92	Fine up to $3M and/or up to 5 years imprisonment	Fine up to $5M	Fine and/or up to 20 years imprisonment	Fine
Engaging in a transaction that involves criminal property.	92	Fine up to $3M and/or up to 5 years imprisonment	Fine up to $5M	Fine and/or up to 20 years imprisonment	Fine
Acquisition, use and possession of criminal property.	93	Fine up to$3M and/or up to 5 years imprisonment	Fine up to $5M	Fine and/or up to 20 years imprisonment	Fine
Non-Disclosure by a person in the regulated sector.	94	Fine up to $lM and/or up to 12 months imprisonment	N/A	Fine and/or up to 10 years imprisonment	N/A
Failure to apply enhanced measures in respect of business relationships and transactions with customers domiciled, resident or incorporated in specified territories as defined in section 94A (2).	94A(3)	N/A	Fine up to $3M	N/A	Fine
Non-Disclosure by a Nominated Employee in the regulated sector.	95	Fine up to $1M and/or up to 12 months imprisonment	N/A	Fine and/or up to 10 years imprisonment	N/A
Tipping off	97	Fine up to $1M and/or up to 12 months imprisonment	N/A	Fine and/or up to 10 years imprisonment	N/A
Breach of appropriate consent provision by the Nominated Employee.	99	Fine up to $lM and/or up to 12 months imprisonment	N/A	Fine and/or up to 5 years imprisonment	N/A
Limit on cash transactions	101A	Fine up to $3M and/or up to 3 years imprisonment	N/A	Fine and/or up to 10 years imprisonment	N/A
Offences prejudicing investigation	104	Fine up to $lM and/or up to 12 months imprisonment	N/A	Fine and/or up to 10 years imprisonment	N/A
Failure to comply with the requirements of a disclosure order	112(1)	Fine up to $lM and/or up to 12 months imprisonment	N/A	N/A	N/A

SCHEDULE OF OFFENCES AND PENALTIES (POCA), *contd.*

Offence	Section	Penalty-Parish Court		Penalty-Circuit Court	
		Individual	Body Corporate	Individual	Body Corporate
Makes a false or misleading statement with respect to a disclosure order	112 (3)	Fine up to $lM and/or up to 12 months imprisonment	N/A	Fine and/or up to 5 years imprisonment	N/A
Failure to comply with the requirements of a customer information order	122 (1)	N/A	Fine up to $1M	N/A	N/A
Makes a false or misleading statement with respect to a customer information order	122 (3)	N/A	Fine up to $1M	N/A	Fine
Failure to comply with directions from the Designated Authority and in the provision of additional information	MLP Reg. 3 (7)	N/A	Fine up to $400,000	N/A	N/A
Failure by regulated businesses to establish and implement regulatory controls	MLP Reg. 5 (5)	Fine up to $3M or up to 3 years imprisonment	Fine up to $5M	Fine or up to 20 years imprisonment	Fine
Failure to carry out identification procedures, transaction verification procedures, record keeping procedures of internal control and communication, and required training to prevent money laundering	MLP Reg. 6 (2)	Fine up to $3M or up to 3 years imprisonment	Fine up to $5M	Fine and/or up to 20 years imprisonment	Fine
Failure to include in its records accurate and relevant information on electronic funds transfer	MLP Reg. 9 (3)	Fine up to $1M and/or up to 12 months imprisonment	Fine up to $3M	N/A	N/A
Failure of a branch/subsidiary of a regulated entity to comply with Part V of POCA and POC (MLP) Regs or the higher of the required standard between the jurisdictions where the regulated business is located and that which the branch/subsidiary is located.	MLP Reg. 18 (3)	Fine up to $3M and/or up to 3 years imprisonment	Fine up to $5M	Fine and/or up to 20 years imprisonment	Fine
Regulated entities failing to notify the Competent Authority of its branch/ subsidiary inability to comply with Part V of POCA and POC (MLP) Regs.	MLP Reg. 18 (3)	Fine up to $3M and/or up to 3 years imprisonment	Fine up to $5M	Fine and/or up to 20 years imprisonment	Fine

SCHEDULE OF OFFENCES AND PENALTIES (POCA), *contd.*

Offence	Section	Penalty- Parish Court		Penalty- Circuit Court	
		Individual	Body Corporate	Individual	Body Corporate
Contravention of regulation 7, 7A, 7B, 11, 14, 15, 16 or 17	MLP Reg. 20 (1)	N/A	Fine up to $5M	N/A	Fine
Fixed Penalties	MLP Reg.5 (l), 5(3), 6 (2), 18 (3) 20 (1)	$2,100,000	$3,500,000	$2,100,000	$3,500,000

Schedule of Offences under the Terrorism Prevention Act

Offence	Section	Penalty- Parish Court		Penalty- Circuit Court	
		Individual	Body Corporate	Individual	Body Corporate
Contravention of duty of entities to report provision (Listed Entities Report)	Sec. 15 (7)	Fine up to $1M and/or up to 12 months imprisonment	Fine up to $3M	N/A	N/A
Fine up to $1M and/or up to 12 months imprisonment Failure to report certain transactions (STR)	Sec. 16 (4)	Fine up to $1M and/or up to 12 months imprisonment	Fine up to $3M	N/A	N/A
Unauthorized disclosures	Sec. 17 (5)	Fine up to $2M and/or up to 2 years imprisonment	Fine up to $6M	N/A	N/A
Failure to implement regulatory controls	Sec. 18 (6)	N/A	Fine up to $1M	N/A	N/A
Failure to comply with any requirement or direction issued within the confines of the TPA by the Competent Authority.	Sec. 18A (5)	N/A	Fine up to $3M	N/A	Fine
Contravention of monitoring order or provision of false or misleading information	Sec. 19 (9)	Fine up to $1M	Fine up to $3M	N/A	N/A
Unauthorized disclosure of monitoring order	Sec. 20 (5)	Fine up to $1M and/or up to 12 months imprisonment	Fine up to $3M	N/A	N/A
Failure to comply with examination or production order	Sec. 22	Fine up to $1M and/or up to 12 months imprisonment	Fine up to $3M	N/A	N/A
Contravention of restraint order	Sec. 40 (1)	Fine up to $1M and/or up to 12 months imprisonment	Fine up to $3M	Fine and/or up to 7 years imprisonment	Fine

Schedule of Offences under the UNSCRIA

Offence	Section	Penalty- Parish Court		Penalty- Circuit Court	
		Individual	Body Corporate	Individual	Body Corporate
Failure to determine on a continuous basis whether there is possession or control of assets owned or controlled by or on behalf of a proscribed person or entity.	Sec. 5 (7)	Fine up to $500,000 and/or up to 6 months imprisonment	Fine up to $3M		
Failure to report whether or not there is possession or control of assets owned or controlled by or on behalf of a proscribed person or entity.	Sec. 5 (7)	Fine up to $500,000 and/or up to 6 months imprisonment	Fine up to $3M		
Failure to comply with direction given by the Designated Authority when reporting under section 5 (3) of the Act.	Sec. 5 (7)	Fine up to $500,000 and/or up to 6 months imprisonment	Fine up to $3M		
Tipping off in relation to a report made under section 5 (3).	Sec. 5 (7)	Fine up to $500,000 and/or up to 6 months imprisonment	Fine up to $3M		
Contravention of a UN sanction enforcement law.	Sec. 10 and 11			Fine and/or up to 10 years imprisonment	Fine
Attempting, conspiring, inciting, aiding, abetting, counseling or procuring, the commission of any offence under subsection (1) or (2) of section 10 and 11.				Fine and/or up to 10 years imprisonment	Fine
Providing false or misleading information to a relevant authority in connection with the requirements of a UN sanction law.	Sec. 12 (3)			Fine and/or up to 10 years imprisonment	
Failure to comply with directions given by the designated authority under the Regulations.	Reg. 8 (3)	Fine up to $3M and/or up to 3 years imprisonment	Fine up to $5M		
Failure to comply with requirements or directions issued by the competent authority.	Reg. 9 (4)		Fine up to $3M		Fine

Schedule of Offences under the UNSCRIA, *contd.*

Offence	Section	Penalty-Parish Court		Penalty-Circuit Court	
		Individual	Body Corporate	Individual	Body Corporate
Holding, using, dealing with, or facilitating the use of freezable assets.	Sec. 5 (2)	Fine up to $1M and/or 12 months imprisonment			
Directly or indirectly making a freezable asset available to a designated authority without a written notice granting the permission of the Minister (sec 7).	Sec. 6 (2)	Fine up to $1M and/or 12 months imprisonment	Fine of $3M	Fine or 10 years imprisonment	Fine

PRINTED BY JAMAICA PRINTING SERVICES (1992) LTD., (GOVERNMENT PRINTERS), DUKE STREET, KINGSTON, JAMAICA