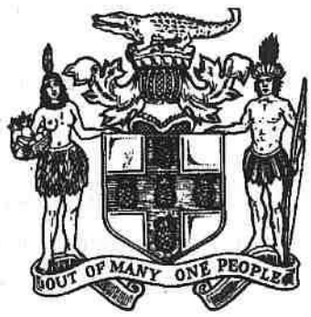
ANTI-MONEY LAUNDERING AND COUNTER TERRORISM FINANCING

TABLE OF CONTENTS



THE

JAMAICA GAZETTE

EXTRAORDINARY

Vol. CXLVII **FRIDAY, SEPTEMBER 20, 2024** **No. 373**

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

DWAYNE HILL, JP (MAJOR)
Governor-General's Secretary and
Clerk to the Privy Council.

GENERAL NOTICES

MISCELLANEOUS

CERTIFICATE OF THE MINISTER OF NATIONAL SECURITY

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING

1: INTRODUCTION AND LEGAL FRAMEWORK

1.1 *Introduction*

1.1.1. In 2015 the Casino Gaming Commission (the CGC) issued the Anti-Money Laundering and Combating the Financing of Terrorism Guidelines for Casinos. Since that time, international efforts at intensifying the fight against money laundering have necessitated amendments in local policies and laws regulating Anti-Money Laundering (AML), Counter Financing of Terrorism (CFT) and Counter Proliferation Financing (CPF). In accordance with Jamaica's international obligations to uphold the legal, regulatory and operational measures implemented and in consequence of the legislative requirements for Competent Authorities to issue Guidelines to their regulated bodies, a review of the CGC's 2015 Guidelines was undertaken.

1.1.2. The primary measures to be implemented in these Guidelines require that stakeholders in the regulated sector, of which casinos are a part:

(a) adopt an improved risk-based approach to their respective AML/CFT/CPF framework;

(b) develop risk profiles for all customers with Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements;

(c) increase the focus on Politically Exposed Persons (PEPs);

(d) report suspicious transactions and entitlement to protection from any liability from such disclosures made in specified cases;

(e) encourage and enforce good record keeping;

(f) implementation of measures to address internal controls, foreign branches and subsidiary obligations; and

(g) implement training of employees and audits of AML/CFT/CPF controls.

1.1.3. These Guidelines have been issued by the CGC, as the Competent Authority, pursuant to section 91(g)(ii) of the Proceeds of Crime Act (POCA) and pursuant to Regulation 20(b) of the Terrorism Prevention (Reporting Entities) Regulations 2010 (TP(RE) Regulations). The objective of these Guidelines is to inform casino operators[1] of their responsibilities under the applicable legislation, as well as to identify best practices in AML, CFT and CPF procedures and systems.

1.1.4. These Guidelines are to be known as the Anti-Money Laundering and Combating the Financing of Terrorism and Proliferation Financing Guidelines for Casinos, 2024, and they supersede the Anti-Money Laundering and Combating the Financing of Terrorism Guidelines for Casinos which were promulgated in 2015.

1.2. *What is meant by proceeds of Crime[2] and Money Laundering?*

1.2.1. *Proceeds of Crime*

Generally, the term "proceeds of crime" refers to all property from which a person benefits directly or indirectly, by being party to criminal conduct[3]. It also includes property that a person gains by spending the proceeds of criminal conduct, for example, if a person uses money earned from drug dealing to buy a car or a house, or spends money gained in a bank robbery to gamble. The latter property referred to is known as criminal property and is defined in section 91 (1) (a) of the POCA as follows—

"(a) property is criminal property if it constitutes a person's benefit from criminal conduct or represents such a benefit, in whole or in part and whether directly or indirectly (and it is immaterial who carried out or benefitted from the conduct);".

1.2.2. *Money Laundering*

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. Section 91(1)(b) of the POCA defines money laundering as—

"An Act which—

(a) constitutes an offence under section 92 or 93;

(b) constitutes an attempt, conspiracy or incitement to commit an offence specified in sub-paragraph (i); or

(c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in sub-paragraph (i);".

There are three (3) acknowledged stages to money laundering: placement, layering and integration. These stages may not all occur and all or some may be separate and distinct or may overlap. The requirements of the criminal or the criminal organization as well as the available mechanisms for facilitating money laundering will determine the use of these three (3) basic stages.

---

[1]That is, the operators of casinos licensed to operate within approved integrated resort developments, within the meaning of the Casino Gaming Act.

[2]The Prevention of Money Laundering and combating the financing of terrorism: Guidance for remote and non-remote casinos, Fourth Edition, January 2019, p6 (The Gambling Commission, UK).

[3]Section 2, POCA.

1.2.3. *Placement*

This is the first stage in the money laundering cycle and where criminals dispose of their cash usually by seeking to place it into the financial system. The criminal is most vulnerable to detection at this stage as banks and other financial institutions have well-developed policies and procedures to detect and prevent money laundering. This has increased the risk of other types of businesses and professions being used to facilitate the disposal of illicit proceeds. Casinos can be targeted because they stock, and legitimately pay out from, a large inventory of cash.

1.2.4. *Layering*

This is the next stage and is where the source of the criminal proceeds is obscured by creating layers of transactions designed to disguise the audit trail to provide anonymity. Once layering commences it becomes difficult to detect money laundering. The layering process often involves the use of different types of entities such as companies and trusts and can take place in several jurisdictions. Casinos may be targeted to facilitate the conversion of cash into other types of assets within and across jurisdictions.

1.2.5. *Integration*

1.2.5.1. This is the final stage in the process where the criminal proceeds reappear as funds or assets which have been legitimately acquired. This is the stage at which money laundering is most difficult to detect. Casinos are often seen as a means of legitimizing illegally obtained money. Casino patrons may attempt to launder money by trying to disguise illegal funds to appear as gambling winnings. This can be done as simply as buying gaming chips at casino gaming tables, participating in very little play and then redeeming the chips for cash or cheques.

1.2.5.2. 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 Financial Action task Force (FATF) Standards—Recommendation 3, the 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 money laundering, 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 money laundering.

1.3. *What is Terrorist Financing?*

1.3.1. Terrorist financing is the process by which funds are provided to an individual or group to fund terrorist activities. Unlike money laundering, such funds can come from both legitimate sources as well as from criminal activity. Funds may involve low-dollar-value transactions and give the appearance of innocence and may also involve 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. However, all the funds are actually transferred to a terrorist group. Funds may come, as well, from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion.

1.3.2. Unlike money laundering, which is preceded by criminal activity, with financing of terrorism there may be fundraising or a criminal activity generating funds prior to the terrorist activity actually taking place. However, like money launderers, terrorism financiers also move funds to disguise their source, destination and purpose for which the funds are to be used to prevent leaving a trail of incriminating evidence, to distance the funds from the crime or the source, and to obscure the intended destination and purpose. The Terrorism Prevention Act (TPA) establishes a number of terrorism offences including engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes.

1.3.3. As with other offences from which a money laundering charge can be derived, the financing of terrorism is a predicate offence for money laundering.

1.4. *What is Proliferation Financing?*

1.4.1. In the context of the regulation of the international financial system and the need to prevent, suppress and disrupt the proliferation of weapons of mass destruction and its financing, the word "proliferation" commonly refers to 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 (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. It includes technology, goods, software, services or expertise.[4]

1.4.2. Using the **Guidance Notes on Counter Proliferation Financing from Gibraltar Financial Intelligence Unit** as a guide, "Proliferation Financing" may be defined as the act of providing funds or financial 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.[5]

1.4.3. Jamaica is not a manufacturer of weapons. It is not an international trade centre nor is it a market of proliferation. It is possible, however, that Jamaica may be used as a transit point for those disguising funds for the purpose of proliferation. Due to its international and domestic obligations, Jamaica supports measures in countering proliferation financing to strengthen the protective framework and contribute to global security. The movement and development of proliferation-sensitive goods can contribute to global instability and if proliferation-sensitive items are deployed, this may ultimately result in the loss of life.

1.4.4. Reporting entities, therefore, need to be aware of the challenges, their responsibilities in this area, and the penalties for breaches.

---

[4]https://www.gfiu.gov.gi/uploads/docs/X86Ru CPF Guidance Notes v1.1.pdf

[5]https://www.gfiu.gov.gi/what-is-proliferation-financing.

1.4.5. There are three (3) stages of Proliferation Financing: program fundraising sources, Disguising the funds; Materials and Technology Procurement.

Program fundraising sources: A proliferating country raises financial resources for in-country costs.

Disguising the funds: The proliferating state moves assets into the international financial system, often involving a foreign exchange transaction, for trade purposes.

Materials and technology procurement: The proliferating state or its agents uses these resources for procurement of materials and technology within the international financial system.

1.5. *Comparison between Money Laundering, Terrorist Financing and Proliferation Financing*

	Money Laundering	Terrorist Financing	Proliferation Financing
Source of Funds	Internally from within criminal organizations	Internally from self-funding cells (centered on criminal activity)	Often state-sponsored programs but also through fundraising activities by non-state actors
Conduits	Favours formal financial system	Favours cash couriers or informal financial systems such as Hawala and currency exchange firms	Formal financial system preferred up until the point of entry into the Democratic People's Republic of Korea (DPRK), where the money is then taken out in cash in a neighbouring country and carried in to DPRK. Additionally, the use of Distributed Ledger Technology (DLT) has become a widely used mechanism to settle transactions for DPRK.
Detection Focus	Suspicious transactions such as deposits uncharacteristics of customer's wealth or the expected activity	Suspicious relationships such as wire transfers between seemingly unrelated parties	Individuals, entities, states goods and materials, activities
Transaction amounts	Large amounts often structured to avoid reporting requirements	Small amounts usually below reporting thresholds	Moderate amounts
Financial Activity	Complex web of transactions often involving shell or front companies, bearer shares, offshore secrecy havens	Varied methods including formal banking system, informal value-transfer systems, smuggling of cash and valuables	Transactions look like normal commercial activity, structured to hide connection to proliferator or proliferation activities
Money Trail	Circular-money eventually ends up with the person who generated it	Linear—money generated is used to propagate terrorist groups and activities	Linear—money is used to purchase goods and materials from brokers or manufacturers. The money can also move in the opposite direction (i.e. from the broker/manufacturer to the proliferator).

1.6 *International Standards to Prevent Money Laundering, the Financing of Terrorism and Counter Proliferation Financing*

1.6.1. The Financial Action Task Force (FATF) was founded in 1989 by the leading industrial nations at the G7 Paris Summit following the United Nations Convention Against the Illicit Traffic of Narcotic Drugs and Psychotropic Substances (1988 Vienna Convention). It is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.[6] The mandate of FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing of proliferation and other related threats to the integrity of the international financial system. The recommendations made by FATF are intended to be of universal application.

[6]http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Countering-Proliferation-Financing.pdf

1.6.2. As revised in February 2012, FATF has issued Forty (40) Recommendations on the international standard on combating money laundering and the financing of terrorism and proliferation. These are commonly referred to as the FATF Recommendations[7]. FATF has encouraged regional inter-governmental bodies to achieve the global implementation of the FATF Recommendations, one such being the Caribbean Financial Action Task Force (CFATF).

1.6.3. The Caribbean Financial Action Task Force is an organization of states and territories of the Caribbean Basin, including Jamaica, which has agreed to implement the FATF's Recommendations as common countermeasures against money laundering and terrorism financing. The CFATF was established as the result of two (2) key meetings convened in Aruba and in Jamaica in the early 1990's. The Member states of the CFATF have entered into a Memorandum of Understanding by which Members, among other things, agreed to adopt and implement the 1988 UN Convention Against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention). Additionally, the Member Sates endorsed and agreed to implement the FATF Recommendations and to fulfill the obligations expressed in the Kingston Declaration On Money Laundering issued in November 1992. This resulted in the Member States agreeing to adopt and implement any other measures for the prevention and control of the laundering of the proceeds of all serious crimes as defined by the laws of each Member State. Hence the Jamaican Government is committed to implement the FATF Recommendations to combat money laundering and terrorism financing.

1.7. *FATF Requirements for Designated Non-Financial Institutions*

1.7.1. The FATF Recommendations state that Designated Non-Financial Institutions (DNFIs) should be subject to the following:

(a) implementation of AML/CFT/CPF regulatory controls (policies and procedures including training of employees and audits of AML/CFT/CPF 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);

(c) Suspicious Transaction Reporting (STR) requirements (FATF Recommendation 20), and as such are entitled to protection from any liability from such disclosures made, and are 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).

1.7.2. Recommendation 22 of the FATF Recommendations requires countries to regulate certain designated non-financial businesses and professions (DNFBPs) as part of its AML/CFT measures. The effect of this as it pertains to casinos is that the customer due diligence and record-keeping requirements set out in FATF Recommendations 10, 11, 12,15, and 17, apply when a casino's customers engage in financial transactions equal to or above the applicable designated threshold.

1.8. *Immediate Outcome 3 of the FATF Methodology*

Immediate Outcome 3 of the FATF Methodology recognizes the obligations of supervisors to regulate financial institutions, DNFBPs and Virtual Asset Service Providers (VASPs) for compliance with AML/CFT requirements commensurate with their risks. The Outcome requires that the following questions be asked by financial institutions, and these questions may be utilized by the CGC in relation to its licensees:

(a) How well does licensing, registration or other controls implemented by supervisors or other authorities prevent criminals and their associates from holding, or being the beneficial owner of a significant or controlling interest or holding a management function in financial institutions?

(b) How well are breaches of such licensing or registration requirements detected?

(c) How well do the supervisors identify and maintain an understanding of the ML/TF risks in the financial and other sectors as a whole, between different sectors and types of institutions, and of individual institutions?

(d) With a view to mitigating the risks, how well do supervisors, on a risk-sensitive basis, supervise or monitor the extent to which financial institutions are complying with their AML/CFT requirements?

(e) To what extent are remedial actions and/or effective, proportionate and dissuasive sanctions applied in practice?

(f) To what extent are supervisors able to demonstrate that their actions have an effect on compliance by financial institutions?

(g) How well do the supervisors promote a clear understanding by financial institutions of their AML/CFT obligations and ML/TF risks?[8]

1.9. Recommendation 28: Regulation and Supervision of DNFBPs[9]

[7]Ibid.

[8]https://www.fatfgafi.org/content/dam/fatfgafi/methodology/FATF%20Methodology%2022%20Feb%202013.pdf.coredownload.pdf

[9]https://cfatf-gafic.org/index.php/documents/fatf-40r/394-fatf-recommendation-28-regulation-and-supervision-of-dnfbps

1.9.1. As provided in the **Methodology For Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems**, Recommendation 28 relates to the regulation and supervision of DNFBPs which includes casinos. The excerpts that affect casinos are:

(a) Countries should ensure that casinos are subject to AML/CFT regulation and supervision. At a minimum:

(i) Countries should require casinos to be licensed;

(ii) Competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding (or being the beneficial owner of a significant or controlling interest), holding a management function, or being an operator of a casino; and

(b) Casinos should be supervised for compliance with AML/CFT requirements.

1.9.2. *All DNFBPs*

Supervision of DNFBPs should be performed on a risk-sensitive basis, including:

(a) Determining the frequency and intensity of AML/CFT supervision of DNFBPs on the basis of their understanding of the ML/TF risks, taking into consideration the characteristics of the DNFBPs, in particular their diversity and number; and

(b) Taking into account the ML/TF risk profile of those DNFBPs, and the degree of discretion allowed to them under the risk-based approach, when assessing the adequacy of the AML/CFT internal controls, policies and procedures of DNFBPs.

1.10 *United Nations Security Council Resolutions (UNSCR)*

1.10.1. FATF Standards - Recommendation 7 requires countries to implement Targeted Financial Sanctions (TFS) to comply with United Nations Security Council Resolutions (UNSCRs) adopted under Chapter VII of the Charter of the United Nations, relating to the prevention, suppression and disruption of proliferation of weapons of mass destruction and its financing. 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).

1.10.2. The UNSCR 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 transshipment of items that would contribute to WMD proliferation; and

(b) country-specific approach under UNSCR 1718 (2006) and UNSCR 2231 (2015) and their (future) successor resolutions against the Democratic People's Republic of Korea (DPKR)[10] and the Islamic Republic of Iran.

1.10.3. 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.

1.10.4. Casino operators, being part of the regulated sector, are required to immediately freeze—

(a) all funds or other assets that are owned or controlled by the designated person or entity, and not just those that can be tied to a particular act, plot or threat of proliferation;

(b) those funds or other assets that are wholly or jointly owned or controlled, directly or indirectly, by designated persons or entities;

(c) the funds or other assets derived or generated from funds or other assets owned or controlled directly or indirectly by designated persons or entities; as well as

(d) funds or other assets of persons and entities acting on behalf of, or at the direction of designated persons or entities.

1.10.5. Additionally, 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.

1.10.6. Countries should have mechanisms for communicating designations to financial institutions and DNFBPs immediately upon taking such action, and providing clear guidance to financial institutions and other persons or entities, including DNFBPs that may be holding targeted funds or other assets, on their obligations in taking action under freezing mechanisms.

1.10.7. Countries should adopt measures which protect the rights of *bona fide* third parties acting in good faith when implementing the obligations under Recommendation 7.

---

[10]The United Nations Security Council Resolutions Implementation (Asset-Freeze-Democratic People's Republic of Korea) Regulations, 2013 was passed in November, 2013.

1.10.8. Appropriate procedures are to be in place to allow for the delisting of designated persons or entities by the Security Council, where, in the view of the country, they do not or no longer meet the criteria for designation.

1.10.9. 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[11].

1.10.10. Section 3 of UNSCRIA 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 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.

1.11. *Mutual Legal Assistance*

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. 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.

1.12. *The Jamaican Legal Framework*

1.12.1. *Money Laundering*

1.12.1.1. The Proceeds of Crime Act (POCA) and the Proceeds of Crime (Money Laundering Prevention) Regulations (POC (MLP) Regulations), impose duties and responsibilities on businesses in the regulated sector to prevent and detect money laundering. With effect from April 1, 2014, by virtue of the Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013, casinos became Designated Non-Financial Institutions (DNFIs) for the purposes of the POCA, and therefore a part of the regulated sector. This step has been taken to counteract money laundering and terrorist financing and bring Jamaica into compliance with its international obligations to effect such measures, in particular, FATF Recommendation 22.

The POCA represents an all-crimes approach to dealing with money laundering and generally the proceeds of crime. It establishes several money laundering offences including: 1.12.1.2.g:

(a) principal money laundering offences[12];

(b) offences of failing to report suspected money laundering[13]; and

(c) offences of tipping off about a money laundering disclosure, tipping off about a money laundering investigation and prejudicing money laundering investigations.[14]

1.12.1.3. The principal money laundering offences are applicable to all persons whether or not they are regulated under the POCA, however, the offences of failing to report suspected money laundering under sections 94 and 95 apply only to persons in the course of business in the regulated sector. Appendix 1 provides guidance to access the Proceeds of Crime of Act and Amendment to the Second Schedule Order, 2019 under the POCA. Additionally, Appendix 1 outlines the consequences of non-compliance with the POCA. The POCA is comprised of seven (7) parts as follows:

(a) Part I treats with the Assets Recovery Agency provisions. The terms "Assets Recovery Agency" and "Director of the Agency" are clarified. The Financial Investigations Division (FID) of the Ministry of Finance and the Public Service (MoFPS) or any other entity so designated by the Minister by Order, is the Assets Recovery Agency and the Director of the Agency is 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 treats with orders related to the recovery of criminal proceeds, being Forfeiture Orders, Pecuniary Penalty Orders and Restraint Orders. Also addressed is the civil recovery of proceeds, etc. of unlawful conduct;

(c) Part V treats with the issue of money laundering;

(d) Part VI deals with Investigations and this includes Disclosure Orders, Search & Seizure Warrants, Customer Information Orders, Recovery of cash in summary proceedings and Account Monitoring Orders; and

---

[11]See FATF Guidance on Counter Proliferation Financing, February, 2018.
[12]POCA sections 92 and 93.
[13]POCA sections 94, 95 and 96.
[14]POCA section 97.

(e) Part VII deals with matters general in nature such as regulation-making powers under the POCA, Tainted Gifts, Rules of Court, Protection of Persons exercising functions under the POCA.

1.12.1.4. The **POC (MLP) Regulations** set out requirements for persons in the regulated sector pertaining to regulatory controls such as the nomination of an officer in the business to be responsible for the implementation of AML/CFT controls; identification procedures for client identification; verification of the purpose and nature of transactions; record-keeping requirements; independent audits; the vetting of the personal and financial history of employees and the training of employees in the provisions of anti-money laundering laws. The POC (MLP) Regulations also create offences for breaches of the obligations imposed by the Regulations.

1.12.1.5. Several areas of the POC (MLP) Regulations that address Know Your Client (KYC) / Customer Due Diligence (CDD) requirements have been highlighted in this Part.

1.12.2. *Risk Profile*

1.12.2.1. Operators are required to establish a risk profile regarding its operations generally, having regard, for example, to its business products offered, its distribution channels, the national, regional and international environment in which the regulated business operates and the size and nature of its operations.[15]

1.12.2.2. A risk profile, as defined in regulation 7(5) of the POC (MLP) Regulations is a formal assessment made by the regulated business concerned as to the level of risk of money laundering posed to the regulated business by the business relationship or transaction concerned.

1.12.2.3. Additionally, operators are required to establish a risk profile for all business relationships and one-off transactions, with a view to determining the level of risk for each.[16] The basis on which such profiles are established should be guided by the respective risk assessments undertaken by regulated entities. High-risk relationships or transactions include any case where the applicant for business concerned is:

(a) a Politically Exposed Person (PEP);

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

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

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

(e) not the ultimate beneficial owner of the assets concerned in the business relationship or one-off transaction;

(f) a member of such other class or category of persons as the supervisory authority may specify by notice published in the *Gazette*.[17]

1.12.3. *Additional KYC/CDD Requirements*

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

(a) periodic updates of customer information must be carried out at least once every seven (7) years or at more frequent intervals as warranted by the risk profile of the business relationship. This is applicable to existing and new customers;

(b) transaction verification involves ensuring that a transaction indicated and conducted is the one intended by the customer. Such verification must be applied particularly in the circumstances specified in Regulation 7(3) of the POC (MLP) Regulations as follows:

- where a transaction involves cash at/or above the prescribed amount;
- where transactions in a single operation or several operations appear to be linked;
- where wire transfer transactions are being conducted;
- where there is doubt about the veracity or adequacy of previously obtained evidence of identity; or
- where the reporting entity is required to make a report under section 94 or 95 of the POCA.

1.12.3.2. KYC details throughout the payment process and chain must be retained for electronic funds transfers. A regulated business conducting electronic funds transfers must ensure that:

(a) for all the persons involved in the transaction it has the correct name, address and account number (if any);

(b) it has the reference number assigned to the transaction, any other reference numbers and the instructions given in relation to the transfer, the source from which the funds are transferred, and every recipient of the funds transferred[18] (Regulation 9 (1), POC (MLP) Regulations);

(c) it has the identity of the recipient of the funds transferred where the transfer involves an amount exceeding five hundred dollars (US); and

---

[15]Regulation 7A(1)(a), POC(MLP) Regulations.

[16]Regulation 7A(1)(b), POC (MLP) Regulations.

[17]Regulation 7A(2), POC(MLP) Regulations.

[18]Applicable to transfers that exceed US$500.

(d) risk-based policies and procedures are in place for determining whether to execute, reject or suspend the transfer where the identification is not made and verified.

1.12.3.3. 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), POC (MLP) Regulations).

1.12.4. *Reasonable Due Diligence*

1.12.4.1. Casino operators are required by Regulation 7A(3) of the POC (MLP) Regulations to carry out reasonable due diligence in the conduct of every transaction (whether done in the course of a business relationship or as a one-off transaction) to ensure that the transaction is—

(a) consistent with the casino operator's knowledge of the transacting Party, as well as the transacting Party's trade or profession, risk profile and the stated source of the funds involved; and

(b) verified as to the identity of the applicant for business and the source of funds involved.

1.12.4.2. Regulation 7(5) defines "customer information" to include the applicant or 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) as well as any other information used to verify the applicant for business's identity or the nature of the applicant for business's trade, profession or source of funds.

1.12.4.3. Casino operators are prohibited from permitting any person to conduct any transaction with the casino operator by means of a numbered account, an anonymous account or any account in a fictitious name.[19]

1.12.4.4. **These Guidelines are not intended to be substitute for legal advice and nothing in this document should be construed as such. Anyone requiring clarification on the legal issues contained in this document should seek their own independent legal advice. These Guidelines do not relieve casino operators of the obligation to know and comply with AML/CTF/CPF laws.**

1.12.5. *The Terrorism Prevention Act*

1.12.5.1. On November 10, 2001, the Government of Jamaica signed in support of the International Convention for the Suppression of the Financing of Terrorism. The TPA was passed in 2005 and was amended in 2010, 2011, 2013 and 2019. It is an Act with the objective of combatting terrorism and addresses related matters. The Act seeks, among other things, to prohibit all forms of terrorism, all forms of financial transactions aimed at aiding terrorism, provide jurisdiction to prosecute acts of terrorism carried out within Jamaica, and prohibit conspiracies in Jamaica to commit terrorism abroad and provide for appropriate penalties for offenders.

1.12.5.2. Relevant to this part of these Guidelines is section 15 (2) of the TPA which obliges certain entities, including casinos, being a reporting entity under the Act, to 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. Section 2 of the TPA defines a "listed entity" as an entity declared to be a "listed entity" in accordance with section 14 of the TPA. The Supreme Court must be sure that the entity is one that is either—

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

(b) is an entity which the DPP on application for an order declaring the entity to be listed entity under the TPA has reasonable grounds to believe:

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

(ii) is knowingly acting on behalf of, at the direction of, or in association with an entity designated by the UNSC as a terrorist entity; or

(iii) not being an individual, is owned or controlled, directly or indirectly, by an entity referred to in sub-paragraph (i).

1.12.5.3. Section 15 of the TPA requires casino operators to report to the Designated Authority[20] 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 property owned or controlled by or on behalf of a listed entity. If a casino operator is in possession or control of such property it must also report the number of persons, contracts or accounts involved and the total value of the property.

1.12.5.4. Sections 15, 16, 16A and 18 of the TPA impose on casino operators responsibilities of reporting, recording, monitoring, establishing and implementing, all of which are geared at not only assisting the government in determining the risk of money laundering and terrorism in Jamaica but to bolster the security of each casino operator to mitigate the risks of being used in connection with money laundering and the financing of terrorism.

1.12.5.5. Casino operators are required to report all suspicious transactions to the Designated Authority thereby making a Suspicious Transaction Report.[21] A casino operator must, among other things, also—

(a) 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[22];

---

[19]Regulation 16, POC (MLP) Regulations.

[20]TPA, subsections 15(1) and (9). In March 2006 the Minister designated the CTD of the FID the Designated Authority for the purposes of reporting obligations and other specific obligations outlined at sections 15-18 of the TPA. Section 15 TPA has been amended to indicate that the CTD of the FID is the Designated Authority.

[21]Section 16, TPA.

[22]Section 18, TPA.

(b) establish and implement programmes, policies, procedures and controls;

(c) establish programmes for training of employees on a continuous basis, for enabling them to fulfill their duties under the TPA; and

(d) designate a Nominated Officer at management level who should, as part of his duties, arrange for independent audits to ensure that compliance programmes are effectively implemented.[23]

1.12.5.6. As an additional measure, section 16A of the TPA was introduced for reporting entities to be exceptionally careful in business relationships and transactions with any customers resident or domiciled, or in the case of a body corporate, incorporated, in a specified territory.[24] The reporting entity, in this regard, should—

(a) apply enhanced due diligence procedures[25];

(b) ensure that the background and purpose of all such relationships and transactions are examined;

(c) ensure that the findings from the two previous paragraphs are set out in writing and made available, upon request, to the designated authority or the competent authority concerned, as the case may require; and

(d) limit those business relationships and one-off transactions, in accordance with enhanced terrorist financing counter-measures set out in regulations made under the TPA.

1.12.6. *The Terrorism Prevention (Reporting Entities) Regulations*

1.12.6.1 The Terrorism Prevention (Reporting Entities) Regulations, 2010 (the TP (RE) Regulations) outline the operational procedures that must be maintained by reporting entities, particularly for the commencement of a business relationship or conducting a one-off transaction. These regulations largely mirror the POC (MLP) Regulations and require casino 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 (4) months as to whether or not the reporting entity is holding property etc. In respect of a listed entity (Listed Entity Report).

1.12.6.2 *These Guidelines are not intended to be a substitute for legal advice and nothing in this document should be construed as such. Anyone requiring clarification on the legal issues contained in this document should seek their own independent legal advice. These Guidelines do not relieve casino operators of the obligation to know and comply with AML/CTF/CPF laws.*

1.12.7. *Other Relevant Legislation*

1.12.7.1.1. 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 MoFPS. The Chief Technical Director (CTD) of the FID or such other person as may be designated by the Minister by order, is the Designated Authority to receive reports under the POCA (section 91(l)(h)), the TPA (section 15) and The United Nations Security Council Resolutions Implementation Act (UNSCRIA) (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.

1.12.7.2. 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. The FID also has the power to disclose to any authorized entity listed within sections 137A (4) of the POCA and 18B (4) of the TPA, 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.

1.12.7.3. Other relevant legislation pertaining to the proceeds of crime and which will assist in determining whether a person has a criminal lifestyle are as specified in the Second Schedule to the Proceeds of Crime Act (excluding those earlier mentioned), the Dangerous Drugs Act, 1948, the Offences Against the Person Act, Firearms Act, Forgery Act, Copyright Act, Patents Act, Larceny Act, Child Pornography (Prevention) Act and the Sexual Offences Act.

1.12.7.4. Other legislative enactments indirectly related to the prevention of money laundering, terrorism financing and proliferation financing are: the Extradition Act, 1991) the Firearms Act, 1967, the Mutual Assistance (Criminal Matters) Act, 1995, the Sharing of Forfeited Property Act, 1999, the Criminal Justice (Suppression of Criminal Organization) Act, 2014, the Law Reform (Fraudulent Transaction) (Special Provisions) Act, 2013, the Cyber Crimes Act, 2015. Other legislation relating to fraud, dishonesty, and corruption would also fall into this category.

1.13. *Who Comprises the Regulated Sector?*

1.13.1. The Fourth Schedule to the POCA explains which businesses fall in the regulated sector. Such a business is one which is—

(a) a financial institution or an entity that has corporate responsibility for the development and implementation of group-wide anti-money laundering, or terrorism financing prevention, policies and procedures for the group of companies of which the entity forms a part, or

(b) a designated non-financial institution (DNFI).[26]

---

[23]Ibid.

[24]This is a territory specified in a list, published by the notice in the *Gazette*, by the designated authority as being a territory in respect of which there is a greater associated risk of money laundering or terrorist financing.

[25]These are such enhanced due diligence procedures that are prescribed pursuant to section 47 which is the regulation-making section.

[26]This is pursuant to the amendment of paragraph 1(1)(a) of the Fourth Schedule of the POCA by Act 26 of 2013.

1.13.2. A financial institution is—

(a) a bank licensed under the Banking Act;

(b) a financial institution licensed under the Financial Institutions Act;

(c) a building society registered under the Building Societies Act;

(d) a society registered under the Co-operative Societies Act;

(e) a person who—

(i) engages in insurance business within the meaning of the Insurance Act; or

(ii) performs services as an insurance intermediary within the meaning of the Insurance Act (but does not include an insurance consultant or an adjuster);

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

(g) a person licensed under the Securities Act as a dealer or investment adviser;

(h) approved money transfer and remittance agents and agencies;

(i) the National Export Import Bank of Jamaica; and

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

1.13.3. A DNFI is a person who is not primarily engaged in carrying on financial business and is designated by the Minister of National Security as a non-financial institution pursuant to paragraph 1(2) of the Fourth Schedule of POCA.

1.13.4. With effect from April 1, 2014, and for the purpose of POCA, casinos became Designated Non-Financial Institutions (DNFIs) pursuant to the Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013.

1.14. *Why Casinos should be regulated*

1.14.1. In evaluating risks and vulnerable activities, FATF has found casinos to be highly susceptible to money laundering and terrorism financing. Historically, casinos have been found to be susceptible to AML/CFT in three (3) areas:

1.14.1.1. *Ownership/Investment*

In the absence of strong regulatory oversight, the investment of illegally generated funds is highly likely. Criminal elements have long used investments into casinos as a vehicle to both legitimize illegally obtained money and to further illegal activities by using casinos to launder money, skim and divert casino profits and other ancillary crimes. If the background of the owners/investors and the financial arrangements to build and equip a casino are not thoroughly investigated, money can easily be laundered by owning a casino. Since casinos operate with cash it is easy to justify large cash deposits into commercial banks from a casino. Casino deposits to banks may include funds from other activities at the casino such as food and beverage sales, hotel room rentals, entertainment venues or shops owned by the casino. This commingling of the deposit may also include other unrelated funds being laundered.

1.14.1.2. *Patrons*

Casino patrons may attempt to launder money by trying to disguise illegal funds to appear as gambling winnings. This may be done, for example, by exchanging small denomination currency, such as would be common in drug transactions, for large denomination currency to facilitate the transporting of money. This could be done by purchasing chips or tokens with small bills and then redeeming them for larger bills. Further, if there are inadequate AML/CFT regulatory standards, a patron could convert disguised winnings into a casino cheque or direct a wire transfer to a bank. Many of these types of transactions can be done by multiple individuals or in small amounts in a further attempt to hide the nature of the transaction.

1.14.1.3. *Employees*

Casinos are also susceptible to money laundering threats from individual employees or groups of employees who may conspire with patrons to facilitate transactions going undetected. This could include employees intentionally failing to adhere to regulations or internal control procedures. Employees could also destroy documents and transaction reports or falsify player gambling records to justify the accumulation of chips or machine credits. Employees may also conspire with management in areas of counting money, bank deposits and accounting for transactions. With employees conspiring with owners and/or patrons, there are any number of possible ways to launder money.

Appendix 3 of these Guidelines provides a list of **Possible Methods of Money Laundering using Casino Operations and** case studies in respect of each one.[27]

1.15. *The Role of the Casino Gaming Commission (CGC)*

1.15.1. The Casino Gaming Commission (the CGC) was established by the Casino Gaming Act, 2010[28] (the CGA), as the body charged with the power to grant casino licences as well as to be the regulatory body for casino gaming in Jamaica. Its functions[29] are to:

(a) regulate and control casino gaming in Jamaica;

(b) approve systems of controls for, and administrative and accounting procedures in, casinos in order to ensure integrity and fairness in casino gaming;

[27]Taken from http://www.fiusrilanka.gov.lk/docs/Training/2018/2018.08.01 AMLCFT Obligations DPMS.pdf
[28]Section 5.
[29]Section 6.

(c) conduct investigations into the operation of casinos and the holders of specified offices;

(d) institute measures and controls to—

(i) protect the vulnerable, including children, from any harm or exploitation arising from casino gaming;

(ii) limit opportunities for crime or any disorder associated with casinos;

(iii) facilitate responsible casino gaming; and

(iv) prevent money laundering and the financing of terrorist activities in relation to casino gaming.

1.15.2. In exercising its functions, the Commission must ensure delivery of the licensing objectives and be guided by such principles as:

(a) regulating casino gambling in the public interest;

(b) regulating in a transparent, accountable, consistent and targeted manner;

(c) assessing risk led by the evidence, relevant information and best regulatory practice in the light of international experience;

(d) consulting widely and effective use of resources.

1.16 *Powers of the Casino Gaming Commission as Competent Authority*

1.16.1. As the Competent Authority, the role of the CGC is to monitor and ensure that casino operators remain compliant with the provisions of the CGA as well as to issue Guidelines to casino operators.

1.16.2 The CGA gives the CGC powers to investigate the suitability of applicants and to maintain a rigorous licensing application procedure.[30] In particular, the CGC will take a serious view of all relevant offences committed by all applicants for licences. Applicants must prove themselves fit and proper persons to be concerned or associated with the management or operation of a casino. In addition, an applicant is disqualified from being granted a licence if it or any of its associates has been convicted of a specified offence.[31] A specified offence is defined in the Act to include offences including money laundering.

1.16.3. Further, the CGC is authorized to review licences[32] where it suspects that a breach of any licensing condition or any regulations made thereunder, or any other enactment, has been committed by the casino operator. Breach of the conditions includes, but is not limited to, the conviction of the casino operator or any of its associates of specified offences in any jurisdiction as well as the suspension, revocation or surrender in any other jurisdiction of any licence or authorization granted to the casino operator or any of its associates to conduct gaming activities in that jurisdiction which is equivalent or similar to casino gaming under the Act.[33]

1.16.4. Breach of licensing conditions may result in regulatory or criminal sanctions.

1.16.5. Disciplinary actions against a casino operator can take the form of:

- issuing a letter of warning, admonishment, censure or reprimand;
- revocation or suspension of a casino gaming licence; or
- variation of the terms of a casino gaming licence.[34]

1.16.6. Disciplinary action can arise where a casino operator, a person in charge of the casino, an agent of the casino operator or a casino employee has contravened any Act or any regulations relating to money laundering or the financing of terrorist activities.[35]

1.16.7. The CGC is also authorized to give a casino operator written directions relating to the conduct, supervision or control of operations in the casino and the casino operator shall comply with such directions.[36] The direction may require the casino operator to adopt, vary, cease or refrain from any practice in respect of the conduct of casino operations.[37] Where a casino operator fails to comply with a direction given he shall be liable on summary conviction in a Parish Court.[38]

1.16.8. The POCA and TPA extend the functions of the CGC as Competent Authority. Subsections (1) and (2) of section 91A of the POCA and section 18A of the TPA give the Competent Authority functions for the purpose of ensuring that any business in the regulated sector, which that Competent Authority is responsible for monitoring, operates in compliance with the aforementioned Acts and any regulations made thereunder. These functions generally address the power to—

(a) establish measures to carry out, or direct a third party to carry out, such inspections or verification procedures as may be necessary;

(b) issue directions to any of the businesses within its regulated sector ("business concerned") and such directions may require the business to take measures for the prevention or detection of, or reducing the risk of, money laundering or terrorist financing;

---

[30]Section 14.
[31]Section 15(1)(c).
[32]Section 20.
[33]Third Schedule (c) and (e).
[34]Section 27.
[35]Section 27(1)(b)(ii) CGA.
[36]Section 38(1) CGA.
[37]Section 38(3) CGA.
[38]Section 38(5) CGA.

(c) 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) share information, pertaining to any examination conducted by it with another competent authority, supervisory authority or the designated authority, or an authority in another jurisdiction exercising functions similar to those of the authorities just mentioned. That information to be shared should not be the type that is protected from disclosure by the Act or any other law, and may be subject to terms and conditions that may prevent disclosure referred to earlier and secure against the compromising or obstruction of an investigation in relation to an offence under the Part V of POCA or any other law;

(e) require the businesses concerned, where this is not already a requirement whether under law or otherwise, to register with the Competent Authority such particulars as may be prescribed and to make such reports to the competent authority in respect of such matters as may be specified. The procedure for requiring the businesses concerned to do these actions should have been in a notice in writing to those businesses;

(f) while exercising its functions, continually assess the risks of money laundering and terrorist financing, relating to the business in the regulated sector and tailor its activities (including any directions or requirements that may be issued, or measures or procedures that may be established) under the respective Acts accordingly.

1.16.9. *The Supervisory Authority*

1.16.9.1. The Fourth Schedule of POCA designates the BOJ and the FSC as supervisory authorities for the purposes of POCA. In particular, as Supervisory Authority, the BOJ preserves general oversight of the financial system. The Supervisory Authority can issue relevant guidance that may be considered in determining whether an offence has been committed by a business (including Designated Non-Financial Businesses and Professions) in the regulated sector under section 94 or 95 of the POCA. The Supervisory Authority can also by notice published in the *Gazette* require that businesses in the regulated sector pay special attention to all business relationships and transactions with customers resident or domiciled in a territory or territories specified by the Supervisory Authority.[39]

1.17. *Status of these Guidelines*

1.17.1. These Guidelines are issued by the CGC in its capacity as the Competent Authority with respect to casino gaming in Jamaica, and are for the use and benefit of casino operators. The purpose of these Guidelines is to:

(a) outline the legal framework for AML/CTF/CPF requirements and systems across the casino gaming sector;

(b) summarize the requirements of the relevant laws supporting AML/CTF/CPF and how they may be implemented in practice;

(c) indicate good industry practice in AML/CTF/CPF procedures through a proportionate risk-based approach; and

(d) assist casino operators to design and implement the policies, procedures and controls necessary to mitigate the risks of being used in connection with money laundering, the financing of terrorism and the financing of proliferation.

1.17.2. These Guidelines represent the CGC's view of the effective measures that casino operators should follow to prevent and detect money laundering. While the Guidelines focus primarily on the relationship between casino operators and their customers, and the money laundering risks presented by transactions with customers, operators should also give due consideration to the money laundering risks posed by their business-to-business relationships, including any third parties with whom they contract.

1.17.3. These Guidelines have been approved by the Minister and published in the *Gazette*. In accordance with section 94 (7) of the POCA, the Court is required to consider compliance with its content in assessing whether a person committed an offence under that section or under section 95 of the POCA. In the event of any inconsistency between the provisions of these Guidelines and the POCA, the TPA, the UNSCRIA and the Regulations under those Acts, the provisions of the Acts and/or their Regulations prevail.

1.17.4. ***These Guidelines are not intended to be a substitute for legal advice and nothing in this document should be construed as such. Anyone requiring clarification on the legal issues contained in this document should seek their own Independent legal advice. These Guidelines do not relieve casino operators of the obligation to know and comply with AML/CTF/CPF laws.***

2. *The Guidelines*

2.1. *Introduction*

2.1.1. The law concerning money laundering is based on the general and wide-ranging prevention and detection of the use of any proceeds of crime, the prevention and detection of terrorist financing, and for some businesses (including casinos) the more specific requirements of the business and its employees to have policies, programmes and procedures in place covering the risks it faces from money laundering.

2.1.2. Money laundering is a term that is often misunderstood. It is defined in section 91 of the POCA and covers wide-ranging circumstances involving any activity concerning the proceeds of any crime. This includes:

(i) trying to turn money raised through criminal activity into 'clean' money (that is, classic money laundering);

(ii) possessing or transferring the benefit of acquisitive crimes such as theft and fraud, and funds generated from crimes like tax evasion;

[39]Section 94A, POCA.

(iii) possessing or transferring stolen goods;

(iv) being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property; and

(v) criminals investing the proceeds of their crimes in the whole range of financial products.

2.1.3. Using money in casinos (regardless of the amount) that is the proceeds of any crime can amount to money laundering if the person using or taking the money knows or suspects that it is the proceeds of crime. Money laundering offences can be committed by both the customer and casino employees, depending on respective levels of knowledge or suspicion.

2.2. *Risk Based Approach (AML/CFT/CPF)—The Supervisory Regime of the Casino Gaming Commission*

2.2.1. In carrying out its regulatory/supervisory role of the casino gaming sector, the CGC has adopted a risk-based approach in conducting its AML/CFT/CPF 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.

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

(a) the size of the casino operation;

(b) the degree of ML/TF/PF risks; and

(c) the level of compliance within the sector.

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

(a) the successful exclusion of criminals and their associates from holding or being the beneficial owner of a significant interest or holding a management function in the casino 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 casino;

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

2.2.4. Supervisory Examination Framework

2.2.4.1. The CGC's supervisory examination framework includes the following:

- 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 CGC or through a third party;
- off-site monitoring tools include questionnaires on the policies, programmes, procedures, risk monitoring and reporting systems in place at the businesses;
- on-site assessment tools include assessing the adequacy of AML/CFT/CPF controls;
- officers engaged in AML/CFT/CPF inspections are to be adequately trained and have up-to-date knowledge of AML/CFT/CPF issues;
- in addition to supervision at an individual operator's entity, where appropriate, risk-based assessments will be conducted across all or part of the casino gaming sector in a thematic approach;
- where feasible, efforts will be made to take risk-sensitive measures to inspect or review; and
- where necessary, the CGC will conduct follow-up and special examinations.

2.2.4.2. The major off-site monitoring tool utilized by the CGC is a self-assessment questionnaire that will be sent to licensees 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.

2.2.4.3. Other off-site monitoring tools that will be deployed by the CGC are:

- thematic reviews where a particular grouping of operators will be required to submit information on a particular area, for instance, customer identification measures;
- meetings with the Nominated Officer and other senior staff;
- interviews; and
- reviews of internal and external AML/CFT/CPF Audit Reports.

2.2.4.4. The CGC's examination process will include an assessment of the adequacy of an operator's AML/CFT/CPF policies, programmes, procedures and controls, the licensee's compliance with these policies, programmes, procedures and controls as well as the applicable legislation and the Guidelines. Accordingly, the AML/CFT/CPF oversight of licensees by the CGC is to:

- assist with understanding each operator's AML/CFT/CPF risks;

- allow for a more targeted assessment of the adequacy and appropriateness of an operator's own risk assessments and AML/CFT/CPF policies and procedures; and
- facilitate the collection of data that will enable the CGC's broader participation in the country's risk-based assessment.

2.2.4.5. Operators should be aware that as the Competent Authority, the CGC can have independent interaction with the Designated Authority or an authority of equivalent jurisdiction, regarding the compliance of a business with its obligations under the applicable legislation. An 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.

2.2.5. *Risk-based Approach (AML/CFT/CPF) - Casinos*

2.2.5.1. Under the FATF Forty (40) Recommendations, 2012, 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/CPF policies. This national risk assessment will therefore inform the overall national AML/CFT/CPF strategy and framework for a country and the implementation of appropriate risk-based measures for the relevant sectors within the country.

2.2.5.2. 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.

2.2.5.3. The POC (MLP) and TP (RE) Regulations require that each business 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.

2.2.5.4. The POC (MLP) Regulation[40] impose compulsory compliance requirements and a breach can constitute a criminal offence. However, within this legal framework of requirements, casinos have the flexibility to devise policies and procedures which best suit their assessment of the money laundering and terrorist financing risks faced by their business. The Regulations require a policy and procedure in relation to risk assessment and management.[41]

2.2.5.5. Operators are already expected to manage their operations with regard to the risks posed to the licensing objectives in the Act, and measure the effectiveness of the policies and procedures they have put in place to manage those risks. The approach to managing the risks of the operator being used for money laundering or terrorist financing is consistent with the existing regulatory requirements. The risk-based approach involves a number of discrete steps in assessing the most proportionate way to manage and mitigate the money laundering, terrorist financing and proliferation financing risks faced by the operator. These steps require the operator to:

- identify the money laundering, terrorist financing and proliferation financing risks that are relevant to the operator;
- design and implement policies and procedures to manage and mitigate these assessed risks;
- monitor and improve the effective operation of these controls; and
- record what has been done, and why.

2.2.5.6. A risk-based approach will serve to balance the burden placed on operators and their customers with a realistic assessment of the threat of the operator being misused in connection with money laundering, terrorist financing and proliferation financing. It focuses on the effort where it is most needed and will have most impact. It is not a blanket "one size fits all" approach, and therefore operators have a degree of flexibility in their methods of compliance.

2.2.5.7. A risk-based approach requires the full commitment and support of senior management, and the active co-operation of all employees. Senior management should ensure that the risk-based approach is part of the operator's philosophy and reflected in its policies and procedures. There needs to be a clear communication of the policies and procedures across the operations of the operator, along with robust mechanisms to ensure that they are carried out effectively, weaknesses are identified, and improvements are made wherever necessary.

2.2.6. *Identifying and Assessing the Risks Faced by the Operator*

2.2.6.1. Casino operators need to continually identify, assess and manage these risks, just like any other business risk. They should assess the level of risk in the context of how their business is structured and operated, and the controls in place to minimize the risks posed to their business by money launderers. The risk-based approach means that casino operators focus their resources on the areas which represent the greatest risk. The benefits of this approach include a more efficient and effective use of resources, minimizing compliance costs and the flexibility to respond to new risks as money laundering methods change.

2.2.6.2. The operator should assess its risks in the context of how it is most likely to be involved in money laundering, terrorist financing or proliferation financing. Assessment of risk is based on a number of questions including:

(a) What risk is posed by the business profile and customers using the casino?

(b) What risk is posed to the casino operator by transactions with business associates and suppliers, including their beneficial ownership and source of funds?

---

[40]POC (MLP) Regulation 6.

[41]POC (MLP) Regulation 6(1).

(c) Is the business high volume consisting of many low-spending customers?

(d) Is the business low volume with high spending customers, perhaps who use and operate within their cheque-cashing facilities?

(e) Is the business a mixed portfolio? Are customers a mix of high spenders and lower spenders and/or a mix of regular and occasional customers?

(f) Are procedures in place to monitor customer transactions and mitigate any money laundering potential?

(g) Is the business local with regular and generally well-known customers?

(h) Is there a large proportion of overseas customers using foreign currency or overseas based bank cheques or debit cards?

(i) Are customers likely to be individuals who hold public positions, that is, Politically Exposed Persons (PEPs)?

(j) Are customers likely to be individuals who hold public positions in other countries, that is, PEPs?

(k) Are customers likely to be engaged in a business which involves significant amounts of cash?

(l) Are there likely to be situations where the source of funds cannot be easily established or explained by the customer?

(m) Are there likely to be situations where the customer's purchase or exchange of chips is irrational or not linked with gaming?

(n) Is the majority of business conducted in the context of business relationships?

(o) Does the customer have multiple or continually changing sources of funds (for example, multiple bank accounts and cash, particularly where this is in different currencies or uncommon bank notes)?

(p) Does the customer have multiple or changing addresses?

(q) Has the customer ever presented a fraudulent identity document or failed to provide an identity document repeatedly on request?

(r) Does the customer's behaviour follow a pattern, or is it constantly changing or changed suddenly recently?

2.2.7 *Risk identification (Customers) and Analysis*

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

(a) Customers and other counterparts;

(b) Countries or geographic areas;

(c) Products;

(d) Services;

(e) Transactions;

(f) Delivery channels;

(g) Operating environment, i.e., business size, activities and complexities; and

(h) National and global issues.

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

2.2.7.3. An 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 an operator from undertaking its own assessment of the risks posed to its operations.

2.2.7.4. For the analysis, an 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 money laundering on a frequent basis. In assessing the impact, the operator may conduct an evaluation of the financial impact of the crime itself and from regulatory sanctions; and the reputational damage that may incur.

2.2.7.5. Some of the risks itemized above are explained briefly below.

2.2.7.5.1. *Country or Geographical Risk*

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 other branches of the business itself may constitute a higher level of risk. The factors that may indicate a higher risk include:

- countries or geographic areas subject to sanctions, embargoes or comparable restrictive measures issued, for instance, by the United Nations;
- 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;
- countries or geographic areas identified by credible sources as providing funding for or otherwise supporting terrorist activities;

- countries or geographic areas identified by credible sources as having a high level of corruption, or other criminal activity.

2.2.7.5.2. *Customer Risk*

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

- customers with frequent and unexplained transfer of funds to different institutions and frequent and unexplained movements of funds between accounts in various geographic locations;
- customers where the structure or characteristics make it difficult to identify the true beneficiary;
- customers that use nominees, trusts, family members, third parties etc.;
- customers whose occupations include cash-intensive businesses such as gas stations, supermarkets, wholesales, market vendors etc. or running charities and other non-profit organizations;
- indirect relationships through intermediaries who are unregulated;
- politically exposed persons (PEPs);
- occasional customers that have transactions above a certain threshold.

2.2.7.5.2.2. Deciding that a customer is presenting a higher risk of money laundering, terrorist financing or proliferation financing does not automatically mean that he is a money launderer or a financier of terrorism or proliferation. Similarly, identifying a customer as presenting a low risk of money laundering or terrorist financing does not mean that the customer is definitely not money laundering.

Employees therefore need to remain vigilant and use their experience and common sense in applying the operator's risk-based criteria and rules, seeking guidance from their Nominated Officer as appropriate.

2.2.7.5.3. Many customers carry a lower money laundering or terrorist financing risk. These might include customers who are regularly employed or who have a regular source of income from a known source which supports the activity being undertaken (this applies equally to pensioners, benefit recipients, or those whose income originates from their partner's employment or income).

2.2.7.5.4. Where a customer is assessed as presenting higher risk it will be necessary to seek additional information in respect of the customer. This will help the operator judge whether the higher risk that the customer is perceived to present is likely to materialize. Such additional information may include an understanding of where the customer's funds and wealth have come from.

2.2.7.5.5. If casinos adopt the threshold approach to Customer Due Diligence (CDD), part of the risk-based approach will involve making decisions about whether or when verification should take place electronically. Operators must determine the extent of their CDD measures, over and above the minimum requirements, on a risk-sensitive basis depending on the risk posed by the customer and their level of gambling.

2.2.7.5.6. In order to be able to detect customer activity that may be suspicious, it is necessary to monitor transactions or activity.[42] Monitoring customer activity should be carried out using the risk-based approach, with higher risk customers being subjected to an appropriate frequency and depth of scrutiny, which is likely to be greater than may be appropriate for lower risk customers.

2.2.7.5.7. *Delivery Channels*

The delivery channels should be included in any assessment of customer risk. The extent to which the 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.

2.2.7.5.8. *Transaction, Product and Service Risk*

A comprehensive ML/TF/PF risk assessment must take into consideration the potential risks from the transactions, products and services that the 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:

- specialized services offered to high-net-worth persons (accredited investors);
- services that offer anonymity like wire transfers, online access to accounts etc.;
- new or innovative products or services that are not provided directly by the operator;
- products that involve cash payments or receipt;
- non face-to-face transactions or services; and
- one-off transactions.

2.2.8. *Risk Matrix*

2.2.8.1. In conducting its AML/CFT/CPF risk analysis, the operator should establish whether all identified categories of risks pose a low, moderate, or high risk to the business operations. The 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.

---

[42]POC (MLP) Regulation 7A.

2.2.8.2. 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.

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

2.2.9. *Risk Management*

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

2.2.9.2. 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.

2.2.10. *Role of Management*

2.2.5.1. 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/CPF systems.

2.2.5.2. See Part 2.4 of these Guidelines for more details on Management's responsibilities.

2.2.11. *Policies, Procedures and Controls*

2.2.11.1 Operators must establish and maintain appropriate written risk-based policies, procedures and controls relating to:

- CDD measures and ongoing monitoring;
- reporting;
- record keeping;
- internal controls;
- risk assessment and management;
- training; and
- the monitoring and management of compliance with, and the internal communication of, such policies and procedures.

2.2.11.2. The policies, programmes, procedures and controls must also include specific policies, programmes, procedures and controls that provide for the identification and scrutiny of:

- complex, unusual or large business transactions that are outside of the norm for the business relationship or one-off transaction in question, or unusual patterns of transactions, that have no apparent economic or legal purpose;
- unusual patterns of transactions, whether completed or not, which appear to be inconsistent with the normal transactions carried out by any particular customer with the business.

2.2.11.3. The operator's policies, procedures and controls should also cover:

- the arrangements for the Nominated Officer reporting to senior management;
- the systems for customer identification and verification, including enhanced arrangements for high-risk customers, which includes PEPs;
- the circumstances in which additional information in respect of customers will be sought in the light of their activity;
- the procedures for handling Suspicious Transaction Reports (STRs), covering reporting by employees and transmission to the Financial Investigations Division (FID);
- the mechanisms for contact between the Nominated Officer and law enforcement or FID, including the circumstances in which appropriate consent should be sought;
- the arrangements for recording information not acted upon by the Nominated Officer, with reasoning as to why no further action was taken;
- the monitoring and management of compliance with internal policies and procedures;
- the communication of such policies and procedures, including details of how compliance is monitored by the Nominated Officer, and the arrangements for communicating the policies and procedures to all relevant employees;
- employee training records; and
- supporting records in respect of business relationships, and the retention period for the records.

2.2.11.3. The 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 the sharing of information between branches/ subsidiaries with adequate safeguards on confidentiality and use of the information exchanged.

2.2.11.4. The policies and procedures should enable the 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.

2.2.12. *Review of the ML/TF/PF Risk Assessment*

2.2.12.1. Risk management is dynamic. A money laundering/terrorist financing risk assessment is not a one-off exercise. Operators must therefore ensure that their policies and procedures for managing risks for money laundering, terrorist financing and proliferation financing are kept under regular review.

2.2.12.2. The risk assessment must be updated at least annually, or more frequently depending on the circumstances. This requires the operator to remain up-to-date with ML/TF/PF 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 should be 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.[43]

2.2.13. *Record-Keeping Requirements*

An operator should note that regardless of the level of risks involved, there is no exemption from record-keeping requirements.

2.2.14. *Branches and Subsidiaries/Related Companies*

2.2.14.1. Operators are required to advise their branches/subsidiaries (resident in Jamaica or overseas) of the provisions of the Jamaican AML/CFT/CPF laws together with the provisions of any applicable Guidelines insofar as the dealings of such subsidiaries or branches are affected. Overseas branches are not considered to be legally distinct from their local head office and are therefore subject to Jamaican laws.

2.2.14.2. Each operator is therefore required to assess the AML/CFT/CPF 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/CPF requirements in that jurisdiction fall short of the Jamaican requirements, the operator should ensure that appropriate additional measures to manage the ML/TF/PF risks are developed, documented, implemented and communicated to the CGC.

2.2.14.3. An operator shall ensure that its local branches and subsidiaries implement, and conform to obligations under the POCA, the TPA, the UNSCRIA and attendant regulations, as well as the Guidelines.

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

- the KYC details for customers are well documented (i.e., identification and other customer information as defined under the POC (MLP) Regulations);
- 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 and currency used);
- method of payment (cheque/cash/credit card/debit card/wire transfer and source of funds used to make the payment);
- 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;
- in relation to branch and subsidiary operations in Jamaica, the 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;
- AML/CFT risk-based measures are employed within the parameters of the AML/CFT laws (e.g. processes that include the imposition of transaction limits beyond or below which enhanced or reduced monitoring measures may be applied; and
- the application of measures commensurate with the risk profile of a customer or product etc.).

2.2.14.5. Operators should also give due consideration to the money laundering risks posed by their business-to-business relationships, including any third parties they contract with. The assessment of these risks is based, among other things, on the risks posed to the operator by transactions and arrangements with business associates and third-party suppliers such as payment providers and processors, including their beneficial ownership and source of funds. Effective management of third-party relationships should assure operators that the relationship is a legitimate one, and that they can evidence why their confidence is justified.

[43]Regulation 6(1)(a)(iv)(B) of POC (MLP) Regulations.

2.3. *Customer Relationships*

2.3.1. Casino operators should be mindful that some risk indicators (for example, a pattern of increasing spend or spend inconsistent with the apparent source of income) could be indicative of money laundering, but also equally of problem gambling, or both. There may also be patterns of play (for example, chasing losses) that appear to be indicative of problem gambling that could also be considered to indicate other risks (for example, spend that is inconsistent with the individual's apparent legitimate income could be the proceeds of crime). While patterns of play may be one indicator of risk, casino operators should satisfy themselves that they have asked, or are prepared to ask, the necessary questions of customers when deciding whether to establish a business relationship, maintain the Relationship or terminate the relationship. In summary, it is perfectly plausible that an individual attempting to spend criminal proceeds or launder money could also be a problem gambler, but one does not necessarily follow the other. The responsibility is on the operator to be in a position to understand these dynamics and mitigate any risks to the licensing objectives.

2.3.2. Casino operators are subject to certain provisions of the POCA (including the regulations) and the relevant licence conditions. Operators have the responsibility to comply with the licensing objectives and, therefore, they should carry out appropriate enquiries and assessments to ensure they do so. While the conclusions drawn and actions taken may differ according to whether money laundering and/or social responsibility risks are identified, the effective identification and management of these risks rests upon the ability of casino operators to have a comprehensive knowledge of their customer relationships and for managers to be clear on their responsibilities.

2.3.3. It is also important that the casino operator is able to reconcile information relating to customers' gambling activities in different parts of the business so that they have a more complete picture of the risks posed by the activities of individual customers.

2.3.4. Commercial and business information should be considered for AML as well as social responsibility purposes when transacting with an individual. This should include arrangements for the monitoring of customers with whom a business relationship has been established. For example, information about customer spend can be used by the casino operator to proactively monitor high risk customers in relation to their money laundering risk.

2.3.5. Customer relationships need to be managed proficiently and records should be maintained as to what information was communicated to the customer, why it was communicated and what consi[illegible]ons were made. If players expect that customer interaction is likely should they play with large amounts of money, or for lengthy periods, and such interaction is consistently applied, there would be less reason for players to question or become suspicious of the motives of these interactions. Casino operators may find it helpful to provide their customers with a leaflet which explains why they are being asked questions about their gameplay.

2.3.6. The CGC recognizes that some operators may find their obligations under the POCA and its Regulations challenging, particularly concerning the management of customer relationships. It is incumbent on operators to have policies, programmes, procedures and controls in place to ensure that they comply with all relevant provisions of the POCA, its Regulations and the relevant licence conditions, in particular in relation to CDD, the reporting of money laundering activity by customers and the obtaining of a defence (appropriate consent) where necessary.

2.3.7. Customer relationships for AML purposes consist of three (3) aspects:

(a) the establishment of the business relationship with the customer, including verification of the customer's identity to a reasonable degree;

(b) the monitoring of customer activity, including account deposits and withdrawals;

(c) the termination of the business relationship with the customer.

2.3.8. At all stages of the relationship it is necessary to consider whether—

(a) the customer is engaging in money laundering (including criminal spend);

(b) there is a need to report suspicious activity or seek a defence (appropriate consent); and

(c) any risks posed to the licensing objectives.

2.3.9. *Establishment of business relationship*

2.3.9.1. A business relationship is a business, professional or commercial relationship between a casino operator and a customer which arises out of the business of the casino operator. The operator is expected, at the time when the contact is established, to have an element of duration. Casino operators are advised to interpret this definition widely.

2.3.9.2. A business relationship with a customer of a casino operator is likely to occur when, for example:

- a customer opens an account with the casino operator or becomes a member of a casino (when a membership scheme is operated by the casino); or
- a customer obtains a cheque-cashing facility.

2.3.9.3. A business relationship with a customer of a casino operator may occur when, for example the casino starts tracking a customer's drop/win figures, other than to establish when the customer reaches the approved threshold for CDD.

2.3.9.4. The lists above are not exhaustive and a casino operator will need to form its own view of when contact is established, or circumstances otherwise arise, with a customer from which it expects, or it could reasonably be inferred that it expects, that the relationship with the customer will have an element of duration. The CGC acknowledges that this may not necessarily be the case when a casino operator permits a customer to join a casino loyalty scheme.

2.3.9.5. When establishing a business relationship, casino operators will need to consider the following:

- the potential risk posed by the customer;
- appropriate due diligence checks on the customer; and
- whether it is known or suspected that the customer may launder money (including criminal spend).

2.3.9.6. Where it is known that the customer is attempting to use the casino operator to launder criminal proceeds (including criminal spend), the operator must carefully consider whether he should establish the business relationship, or suspend or terminate the business relationship at the earliest opportunity. In either case, it is recommended that a STR is submitted to the Designated Authority and, where there are funds to be returned to the customer, seek a defence (appropriate consent) to a principal money laundering offence.

There is further discussion of business relationships in Part 2.10 of these Guidelines.

2.3.10. *Customer Monitoring*

2.3.10.1. Where, through their customer profile or known pattern of gambling activity, the customer appears to pose a risk of actual or potential money laundering, the casino operator must monitor the gambling activity of the customer and consider whether further due diligence measures are required. This should include a decision about whether a defence (appropriate consent)[44] should be sought for future transactions (on a transaction by transaction basis), or whether the business relationship with the customer should be terminated where the risk of breaches of the POCA are too high.

2.3.10.2. Casino operators should ensure that the arrangements that they have in place to monitor customers and the accounts they hold across outlets, products and platforms are sufficient to manage the risks to which the operator is exposed. This should include the monitoring of account deposits and withdrawals. Those casino operators that rely heavily on gaming machines should also have practical systems in place to effectively monitor and reconcile customer spend on gaming machines. Any suspicious activity should be reported by means of a STR to the Designated Authority.

2.3.10.3. Once knowledge or suspicion of criminal spend is linked to a customer in one area of the business (for example, gaming machine play), casino operators should monitor the customer's activity in other areas of the business (for example, table games).

2.3.10.4. If the customer's patterns of gambling lead to an increasing level of suspicion of money laundering, or to actual knowledge of money laundering, casino operators should seriously consider whether they wish to allow the customer to continue using their gaming facilities, otherwise the operator may potentially commit one of the principal money laundering offences.

2.3.10.5. Customer monitoring forms part of ongoing monitoring.

2.3.11. *Termination of business relationship*

2.3.11.1. To avoid potentially committing one of the principal money laundering offences, casino operators need to consider ending the business relationship with a customer in the following circumstances:

- where it is known that the customer is attempting to use the operator to launder criminal proceeds or for criminal spend;
- where the risk of breaches to the POCA are considered by the operator to be too high;
- where the customer's gambling activity leads to an increasing level of suspicion, or actual knowledge of, money laundering; or
- where the customer is proven to a reasonable degree of confidence to not have the identity they claim.

2.3.11.2. Additionally, where, in relation to any customer, the casino operator is unable to apply CDD measures, the business relationship with the customer must be terminated and the operator must submit a STR to the Designated Authority where they consider the circumstances to be suspicious.

2.3.11.3. Where the casino operator terminates a business relationship with a customer and they know or suspect that the customer has engaged in money laundering, they should seek a defence (appropriate consent)[45] from the Designated Authority before paying out any winnings or returning funds to the customer.

2.4. *Senior Management Responsibility*

2.4.1. *Introduction*

2.4.1.1. Senior management must be fully engaged in the processes around an operator's assessment of risks for money laundering, terrorist financing and proliferation financing, and must be involved at every level of the decision-making to develop the operator's policies and processes to comply with the Regulations.[46] Disregard for the legal requirements, for example, turning a blind eye to customers spending criminal proceeds or criminal spend, may result in criminal or regulatory action.

2.4.1.2. It is considered best practice that a risk-based approach should be taken to tackling money laundering, terrorist financing and proliferation financing.

2.4.1.3. 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

[44]See paragraph 2.11.8.
[45]See Part 2.11 of these Guidelines on appropriate consent.
[46]POCA (MLP) Regulation 6(1)(b); TPA Regulation 4(1)(b); FATF.

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/CPF systems.

2.4.1.4. An officer of a casino operator which is subject to the Regulations (that is, a director, manager, secretary, chief executive, member of the management committee, or a person purporting to act in such a capacity) who consents to, or connives in, the commission of offences under the Regulations, or where the commission of any such offence is attributable to any neglect on his part, will be individually liable for the offence.

2.4.2. *Obligations on all operators*

2.4.2.1. Senior management should require that the Nominated Officer should compile an annual report covering the operation and effectiveness of the operator's policies and procedures to combat money laundering, terrorist financing and proliferation financing. The Nominated Officer should also be required to periodically provide reports to the senior management, and the board of directors on the effectiveness of the AML/CFT/CPF framework. Where applicable, this report should also speak to compliance levels with directives pertaining to Targeted Financial Sanctions (TFS) notified by the UNSC. In practice, senior management should determine the depth and frequency of information they feel is necessary to discharge their responsibilities. The Nominated Officer may not need to provide the names of suspected persons in any report.

2.4.2.2. The Nominated Officer should compile an annual report covering the operation and effectiveness of the operator's policies and procedures to combat money laundering. In practice, senior management should determine the depth and frequency of information they feel is necessary to discharge their responsibilities. The Nominated Officer may also wish to report to senior management more frequently than annually, as circumstances dictate. The Nominated Officer may not need to provide the names of suspected persons in any report.

2.5 *Training*

2.5.1. The regulations of the POCA and the TPA require that all relevant employees of casinos must be trained regarding the basic provisions of the POCA, the POC (MLP) Regulations, TPA and the TP (RE) Regulations. Operators must ensure that their employees understand the Regulations and apply the operator's policies and procedures, including the requirements for CDD, record keeping and STRs.

2.5.2. One of the most important controls over the prevention and detection of money laundering and financing of terrorism is to have employees who are alert to the risks of money laundering and terrorist financing, and who are well-trained in the identification of unusual activities or transactions which appear to be suspicious. The effective application of even the best-designed control systems can be quickly compromised if the employees applying the systems are not adequately trained. The effectiveness of the training will therefore be important to the success of the operator's AML/CFT strategy.

2.5.3. Operators should devise and implement a clear and well-articulated policy and procedure to ensure that relevant employees are aware of their legal obligations, in respect of the prevention of money laundering and terrorist financing. Additionally, there should be the provision of regular training in the identification and reporting of anything that gives grounds for suspicion of money laundering or terrorist financing.

2.5.4. Operators should also ensure that relevant employees are aware of and understand:

- the money laundering, terrorist financing and proliferation financing risks faced by an operator and each of its casino premises;
- the operator's procedures for managing those risks;
- the identity, role and responsibilities of the Nominated Officer, and what should be done in his absence;
- the potential effect of a breach upon the operator and upon its employees;
- how the casino will undertake CDD;
- how the casino will track customers when CDD is not undertaken on entry to the casino; and
- how PEPs will be identified.

2.5.5. Members of staff must be made aware of their obligations under the POCA, the TPA and the UNSCRIA (including regulations made under these Acts) 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.

2.5.6. Under the POCA, the TPA and the UNSCRIA, individual employees face criminal penalties if they are involved in money laundering, terrorist financing or proliferation financing/holding. The latter being for using or dealing with freezable assets or aiding, abetting, procuring, counselling, conspiring in, or attempting the commission of an offence under regulation 5 or 6 of the UNSCRIA regulations, or making a freezable asset available to a designated entity other than as permitted under regulation 7 of the UNSCRIA Regulations. It is important, therefore, that employees are made aware of their legal obligations, and are given training in how to discharge them.

2.5.7. 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.[47] Under the TPA, a defence of having a reasonable excuse[48] for not making a report in relation to assets held for listed entities or STRs,

[47]See POCA section 94(6).

[48]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.)

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.

2.5.8. Regulation 5(4) of the UNSCRIA Regulations provides that it is a defence against a charge for an offence under paragraph (1) if the person charged proves that the use or dealing was solely for the purpose of preserving the value of the freezable asset.

2.5.9. The employees who would be required to have training in the prevention of money laundering, counter-terrorism financing and counter-proliferation financing, are persons employed in specified offices as defined in the Casino Gaming Act and who are the holders of personal licences issued by the CGC, as well as employees responsible for completing CDD measures.

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

2.5.10.1. *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 Nominated Officer of the business. They must be informed of their personal legal obligation as well as that of the business, to report suspicious transactions. As mentioned, businesses should also institute appropriate screening processes to thoroughly investigate the background, honesty, and integrity of prospective employees.

2.5.10.2. *Front Line Employees*:

The first point of contact of a business 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 reporting systems and procedures of a business to be adopted when a transaction is deemed to be suspicious. Additionally, they must be informed as to the policy of the business for dealing with occasional customers and 'one-off transactions', particularly where large cash transactions are involved.

2.5.10.3. *Employees Opening new Accounts or Approving New Customers*:

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 account opening and customer verification procedures of the business. 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 whether the transaction is proceeded with, or terminated.

2.5.10.4. *Administration/Operations Supervisors and Managers*:

2.5.10.4.1. A higher level of instruction covering all aspects of AML/ CFT/CPF procedures should be provided to persons with the responsibility for supervising or managing staff. Such training must include familiarization with the offences and penalties arising under the POCA, TPA and the UNSCRIA, the procedures relating to monitoring orders, production orders and other court orders, the requirements for non-disclosure and for retention of records, and management's specific responsibility with dealings with customers in accordance with the risk profiles applicable to those customers.

2.5.11. The content of any training, the regularity of training and the assessment of competence following training are matters for each operator to assess and decide in light of the money laundering risks they identify. The CGC will expect such issues to be covered in each operator's policies and procedures.

2.5.12. Ongoing training should be given to all relevant employees at appropriate intervals. Training/education programmes must be designed and implemented on an ongoing basis by operators to ensure employees' awareness of:

- current as well as new and developing AML/CFT/CPF laws, regulations, standards and guidelines being established both locally and internationally;
- their legal obligations and responsibilities to detect and prevent ML/TF/PF;
- new ML/TF/PF techniques, methods, typologies and trends; and
- the AML/CFT/CPF policies and procedures of the business, including proper identification, record-keeping, internal control and communication procedures.

2.5.13. There is no single solution when determining how to deliver training and a mix of training methods may, therefore, be appropriate. Online training systems can provide a solution for many, employees, but this approach may not be suitable for all employees. Classroom training can be more effective in these circumstances.

2.5.14. Compliance with this requirement to train employees is perhaps best achieved in systems that trigger automatic training requirements on the occurrence of certain events e.g.:

- employment;
- promotion/lateral movement to sensitive or frontline duties; or
- expiration of minimum period since the last training session, thereby triggering refresher-training requirements.

2.5.15. 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 a scheduled, standardized style of training.

2.5.16. Casino operators must maintain proper training logs for all AML/CFT/CPF training initiatives to ensure that satisfactory steps are taken to confirm that training of employees occurred. Such steps may include the following:

- 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;
- videotaping of scheduled training sessions (seminar participants must be aware that the session is being taped or recorded in any way);
- delivery of documented certification to employees evidencing satisfactory completion of training session;
- demonstration of knowledge retention of training material, for example, test scores;
- separate verification of the training sessions having taken place by the Nominated Officer; and/or
- Sign off on the sessions taking place by the Board of the casino operator as a part of the audited annual report of the business.

2.5.17. 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 business, job functions and responsibilities. AML/CFT/CPF policies and procedures manual should be readily available to all employees for instance, ensuring:

- such documents are available on internal electronic access (e.g. intranets);
- sufficient copies are placed in resource centres or in-house libraries; and
- the timely circulation of updates and amendments throughout the business network (i.e. head office to branches and representative offices and parent companies to subsidiaries/related companies).

2.5.18. Policy and Procedure manuals, whether paper or electronic, are useful in raising employee awareness and can supplement more dedicated forms of training, but their main purpose is generally to provide ongoing reference rather than being written as training material.

2.5.19. The Nominated Officer should be heavily involved in devising and managing the delivery of such training, taking particular care to ensure that systems are in place to cover all part-time or casual employees.

2.6. *Nominated Officer*

2.6.1. *The Role of the Nominated Officer*[49]

2.6.1.1. The 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) in accordance with the AML/CTF/CPF laws, Guidelines and the conditions of licence of the operator, and the reporting of transactions to the FID. Each operator must designate an officer of the business who performs management functions as its Nominated Officer.[50]

2.6.1.2. Operators must inform the CGC, 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 CGC is to be notified.

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

- is sufficiently senior to allow for reporting to the Board, (or such other governing body) of the business either directly (at Board meetings) or through a Sub-Committee of the Board, on the AML/CFT/CPF compliance of the business;
- requires knowledge of the AML/CFT/CPF laws, framework, global practices and trends that can guide the business in establishing and maintaining the requisite controls, policies and procedures in accordance with the statutory requirements and related framework;
- requires the ability and capacity to undertake the responsibility for ongoing monitoring of the fulfilment of AML/CFT/CPF duties by the business including sample testing of compliance, reviewing exception reports and being the contact point regarding all AML/CFT/CPF issues for internal and external authorities including supervisory authorities or the Financial Investigations Division (FID); and
- is independent of the business/operational lines of the business to allow for an objective assessment and monitoring and enforcement of the compliance of the operations and decision making of the business with its AML/CFT/CPF obligations under the country's framework and with the AML/CFT/CPF policies and procedures of the business.

2.6.1.4. The Nominated Officer is responsible for reporting to the Designated Authority[51] 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/CPF laws and should Consult with the Designated Authority accordingly.

---

[49]Please see Appendix 2 for additional roles of the Nominated Officer.
[50]See POCA (MLP) Regulations, 2007 r. 5(3); TPA section 18(3).
[51]POCA section 95, TPA section 18(3).

2.6.1.5. The policy manual of the regulated business 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 business. 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 measures of the business to address these risks. This report should include:

- An annual overview and evaluation of the overall effectiveness of the AML/CFT/CPF framework of the business, the effectiveness of AML/CFT/CPF measures implemented under each of the various operational areas and/or product and service types, as well as AML/CFT/CPF training exercises completed and initiatives pursued;
- The casino operator's compliance with relevant legislation and these Guidelines in relation to the AML/CFT/CPF reporting obligations of the business, as well as the operator's policies and procedures;
- Particulars of the risk assessment and risk management activities (see Part 2.2 of these Guidelines) including:
    - update on the casino operator's overall relationship with the Designated Authority and general guidance received from that body;
    - advice on any proposed/impending legislative/regulatory AML/CFT/CPF amendments, with an assessment of possible impact on the business with appropriate proposal for the requisite operational changes required for continued compliance.

2.6.2. *Confidentiality Provisions*

2.6.2.1. 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 process and the entity is subject to any investigatory order, for example, an Account Monitoring Order.

2.6.2.2. 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 provide that:

- The requisite systems should be in place by an operator 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;
- The existence of an investigatory order must only be disclosed to other officers or employees within the business, 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 there is compliance with the Order. He 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 constable named within the Order without consulting other employees;
- 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 business apprised of the 'Order' must not disclose the existence of the "Order" to other employees.

2.6.2.3. The role of the Nominated Officer involves the development and implementation of programmes, policies, procedures and controls. A more detailed role of the Nominated Officer may be found in Appendix 2 of these Guidelines.

2.6.2.4. The Nominated Officer is to also be involved in ensuring the training of employees as follows:

- establishing on-going training in respect of AML/CFT/CPF matters and the policies of the operator in respect thereof, and maintaining and reviewing records evidencing such training;
- ensuring that new employees receive appropriate training in respect of AML/CFT/CPF immediately upon assuming employment; and
- advising in respect of proposed or impending changes to AML/CFT/CPF laws, regulations or regulatory guidance.

2.6.2.5. The Nominated Officer has reporting[52] functions that include:

- seeking the consent of the Designated Authority (FID) in respect of transactions in accordance with the requirements of POCA and the POC (MLP) Regulations;
- receiving and evaluating disclosures STR's in respect of suspected money laundering and ensuring timely filing of reports in respect thereof, with the FID;
- providing advice and guidance to employees on the identification of suspicious transactions;
- maintaining files or copies of STR's submitted to the FID in accordance with relevant laws, regulations, regulatory guidance and the policy of the operator;
- providing reports on a regular periodic basis to the senior management or other relevant persons within the operation, on AML/CFT issues; and

[52]Section 95 of the POCA.

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

as well as monitoring functions, including:

- ensuring that record retention requirements and due diligence requirements are in keeping with AML/CFT laws and regulatory guidelines;
- conducting periodic reviews where a STR has been filed and making recommendations to the senior management or other relevant persons within the operation regarding the termination of customer or other business relationships and for the refusal to undertake new business from customers or other persons;
- ensuring reviews of daily transactions in order to identify unusual/potentially fraudulent activities, account excesses, etc.
- ensuring periodic checks in respect of new customers/customer databases against relevant government listings of sanctioned persons/entities and other terrorist watch lists, are performed to ensure that the operator does not/has not entered into relationships with known/suspected terrorists;
- escalating matters of concern to the senior management or other relevant persons within the operation; and
- ensuring that enhanced monitoring is undertaken as required by the law or regulatory guidance, including but not limited to enhanced monitoring for high-risk persons.

Know Your Customer ('KYC') and Customer Due Diligence ('CDD')[53]

2.7.1. *Interpretation*

2.7.1.1. For the purpose of this Part of the Guidelines, the following definitions of terms used shall apply:

"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 casino 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) financial data which has not been updated for eighteen (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 CGC 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;

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

"transaction" refers to all currency transfers including cash-in and cash-out of a casino operator;

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 casino operator to the customer.

2.7.1.2. *General Requirements for Know Your Customer ("KYC") & Customer Due Diligence ("CDD")*[54]

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

(a) occupation and economic activity;

(b) personal financial and business track record;

(c) source of wealth/funds;

(d) contact information;

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

2.7.1.2.2. 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.[55] The CDD must enable a casino operator to know its customer by obtaining information on what the customer does.

2.7.1.2.3. A casino 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.

2.7.1.2.4. Casino 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 casino 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.

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

2.7.1.2.6. Casino operators are prohibited from keeping anonymous accounts, fictitious names or numbered accounts. The reference to "numbered account" in POC (MLP) Regulation 16(2) and TP (RE) Regulation 16(2), means an account that is identifiable solely by reference to the number or numbers assigned to that account.

2.7.1.2.7. In seeking to discontinue the procedures for establishing a business relationship[56] or a transaction started or attempted, or to terminate the business relationship, casino operators should be mindful of the prohibition against tipping off[57] or unauthorized disclosures[58] outlined under sections 97 and 104 of the POCA and section 17 of the TPA. Casino 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 casino operator that an offence is being attempted or has been or is being committed.

2.7.1.2.8. Casino operators should ensure that they have the ability to legally terminate arrangements, transactions or the business relationship, where the casino operator forms 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 business due to the suspected criminal activity.

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

---

[54]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.

[55]FATF Recommendation 10(CDD measures to be taken).

[56]Paragraph 2.3.9 of these Guidelines.

[57]Paragraph 2.3.11 of these Guidelines.

[58]Paragraphs 2.7.1.11 and 2.11.1.2 of these Guidelines on authorized disclosures.

2.7.2. *Updating KYC Records*

2.7.2.1. Casino operators should undertake regular reviews [59] of all existing customers' records (identification and other particulars) to ensure that they remain up-to-date, relevant, consistent with the casino operator's risk profile of that customer and remain subject to appropriate KYC and CDD processes. These reviews should be done at least seven (7) years from the date of the commencement of the relationship and at minimum seven (7) years increments thereafter, or, at more frequent intervals to ensure the accuracy of the information held by the business or as warranted by the risk profile of the customer.

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

2.7.2.3. Reviews[60] should also be necessary under the following circumstances:

- upon the execution (or attempted execution) of a significant transaction;
- upon material changes to customer documentation standards;
- when there is material change in the manner in which the account is operated;
- when, during the course of the business relationship, doubt arises regarding the identity of the customer or the beneficial owner of the account;
- where the casino operator becomes aware at any time that it lacks sufficient information about an existing customer/about the existing business relationship with a customer;
- 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;[61]
- where transactions carried out in a single operation or in several operations appear to be linked;
- where a transaction is carried out by means of wire transfers;
- where there is any doubt about the veracity or adequacy of previously obtained evidence of identity; or
- where the casino 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).

2.7.2.4. If, during the course of the updating exercise or any time after the business relationship has commenced, the casino 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 casino operator, unreasonably withheld, then the casino operator must take steps to terminate the relationship[62] 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[63] and should also be available to the auditors (internal and external) where applicable, of that business. In such cases, those accounts should be legally terminated unless a direction/ request to the contrary is received from the Designated Authority.

2.7.2.5. Where there are gaps in the KYC database[64] casino 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:

- omissions in the database of KYC information that are required under the law or AML/CFT/CPF regulatory framework (particularly where this occurs in relation to customers that are classified as 'high risk');
- 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 casino operator's records should be treated as incomplete and the customer name must be obtained and verified;
- adjusting records to reflect changes to the KYC particulars such as, name change by marriage or deed poll;
- changes in the current permanent address; or
- changes in employment/business trade and/or profession; and identification updates.

2.7.2.6 Casino operators should ensure that the records reflect the current information, and devote attention to correcting errors or addressing inaccuracies.

2.7.2.7 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.

---

[59]POCA (MLP) Regulations, 2007-r. 7(1)(c) and (d) and r. 19; TP (Reporting Entities) Regulations, 2010 (r. 5 and 21).
[60]POC (MLP) Regulations, 2007-r. 7(2)(b) and 7(3); and TP (Reporting Entities) Regulations, 2010 (regulations 5 and 6(2)(b)).
[61]POCA speaks to the following prescribed amounts: a TTR limit for cash transactions (see regulation 3 of the POC (MLP) Regulations (not applicable to casino operators) and cash transaction limits (see POCA section 101A). No amounts are prescribed under the TPA or regulations thereunder.
[62]POC (MLP) Regulations, 2007 regulation 7(1)(b) and TP (Reporting Entities) Regulations, 2010 regulation 5(a)(iii).
[63]Regulation 14(4) of the POC (MLP) Regulations, amended 2013 (NB. Regulation 14 of the TP (RE) Regulations. These regulations speak to the record-keeping obligation of reporting entities).
[64]The Law indicates that for accounts that pre-date the prescribed date of 29th day of March, 2007 only identity updates (which include address verification) are required (regulation 19-POC (MLP) Regulations amended 2013.

2.7.3. *Identification of Natural Persons*

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

- valid driver's licence, issued by the authorities in the country in which the person is resident;
- valid passport issued by the authorities in the country in which the person is resident; or
- valid voter's identification card.

2.7.3.2. The following information is required to satisfy basic KYC requirements for natural persons and any customer information order served on the casino operator:[65]

- Customer Identification Information;
- Customer Account number and transaction number;
- Date on which the individual began to hold the account;
- date on which the individual ceased to hold the account;
- transaction date and description of transaction type (e.g. deposit/cash-in, winnings);
- source of funds that will be used in the transaction or used to access the service offered by the casino operator;
- source of wealth;
- occupation or economic activity generating the source of income;
- business and personal contact details; and
- 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.

2.7.4. Customer Identification for Natural Persons (Resident in the Jurisdiction or Not)

2.7.4.1. The following information[66] must be obtained from all prospective customers:

- full true name and other names/aliases used;
- correct permanent address, including postal address (if different from the permanent address);
- date and place of birth;
- nationality;
- Taxpayer Registration Number (TRN) or other reference number;
- contact numbers (work, home, mobile/cell).

2.7.4.2. Under the POC (MLP) Regulations, customer information includes the TRN or other reference number. The CGC 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.

2.7.5. *Address Verification Documents*

The permanent address of the applicant for business should be verified by an independent and reliable source. The following methods may be used:[67]

- recent bill from a utility provider such as a telephone, internet, cable, water or electricity service provider;
- telephone directory;
- Voter Identification Card; or
- Driver's Licence.

2.7.6. *Verification of CDD, KYC and Transaction Details*

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

- requesting a utility bill in the name of the customer with its date not past three (3) months, for example: electricity, telephone, water, cable and internet;
- checking a local telephone directory;
- checking with the Electoral Office of Jamaica;
- Driver's Licence which should be verified through Tax Administration Jamaica (TAJ); or

---

[65]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 trust as per regulation 13(1)(c).

[66]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.

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

- passports which should be verified through the Passport, Immigration and Citizen Agency ('PICA') or other issuing authority.

2.7.6.2. 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.

2.7.7. Self-Employed Persons and Sole Proprietors

2.7.7.1. Casino 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:

- identification and other details as outlined in paragraphs 2.7.3, 2.7.4 and 2.7.5 of these Guidelines; 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);
- 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); and
- Tax Compliance Certificate (TCC)[68] or other equivalent official confirmation from the relevant tax authorities of compliance with income tax obligations.

2.7.8. *Customers Resident Overseas*

2.7.8.1. Casino operators occasionally open accounts or form business relationships with persons who reside overseas. Casino 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.

2.7.8.2. 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, casino operators should have specific and adequate measures to mitigate the higher risk.

2.7.8.3. These measures to mitigate risk may include:

- certification of documents presented;
- requisition of additional documents; and
- independent verification of documents by contacting third parties.

2.7.8.4. Casino operators are required to ensure that, among other things, a casino operator's AML/CFT/CPF measures include paying special attention to all business relationships and transactions with any customer resident or domiciled in a territory specified in a list of applicable territories published by notice in the *Gazette* by a supervisory authority.[69] For the purposes of these Guidelines, the jurisdictions targeted for this special attention include jurisdictions flagged by:—

- FATF;
- One (1) or more of the other eight (8) FATF Styled Regional Bodies (FSRB);
- UNSC; and
- 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.

2.7.9. *Natural Persons Resident Overseas*

The identification and KYC requirements for natural persons resident in Jamaica also apply to natural persons resident outside of Jamaica. Casino operators are required to obtain the same identification documentation or their equivalent for prospective customers' resident outside of Jamaica.[70]

2.7.10. Verification of Identification Details Post-Commencement of Business

2.7.10.1. POC (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 casino 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—

- the nature of the proposed business relationship;
- the nature of the transaction(s) contemplated;

---

[68]TCC (or equivalent confirmation of tax compliance) valid for one (1) year can be obtained provided the taxpayer's information in the database of Tax Administration Jamaica can support the issuing of a TCC or other such confirmation for that period.
[69]Section 94A, the POCA.
[70]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.

- the geographical location of the parties;
- 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 interrupt the normal conduct of business); and
- assessment of the risks to the business, if it proceeds without confirmation of the customer's identification.

2.7.11. *Transaction Verification*

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

- ensuring that the customers have tendered evidence of the requisite instructions pertaining to the transaction at hand;
- confirming 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.; and
- confirming the consistency of the transaction being conducted with transaction patterns for the account history.

2.7.11.2. 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.

2.7.11.3. 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.[71] A casino operator should also ensure that evidence of transaction verification it has undertaken is documented and retained. This should be 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 casino operator.

2.8. *Simplified and Enhanced Identification and KYC Requirements*

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.[72] 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.[73]

2.8.1. *Simplified Measures*

2.8.1.1. Where a casino operator has determined that a business relationship or one-off transaction is low risk, the casino operator may, with the written approval of the Competent Authority, apply simplified due diligence procedures.[74]

2.8.1.2. In assessing whether there is a low degree of risk, casino 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.

2.8.1.3. Prior to the application of Simplified Due Diligence measures casino operators must meet the requirements set out in paragraph 2.8.1.4 below and obtain written approval from the Competent Authority.

2.8.1.4. *Casino operators must meet the following requirements*:[75]

- by conducting an assessment, as discussed in paragraph 2.2.7.5.2 of these 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;
- by documenting the assessment methodology (including data source; active periods covered by the assessment; basis for methodology and findings);
- by 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);
- by 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;
- by demonstrating a satisfactory level of compliance with the POCA/ TPA/UNSCRIA, regulations made under these Acts and all other laws concerning ML/TF/PF; and
- with the agreement of the Designated Authority, the matter is an appropriate one for the application of simplified due diligence procedures.

---

[71]POC (MLP) Regulation 14(4).
[72]FATF Guidance Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion, February 2013–Paragraph 68.
[73]Revised FATF Recommendations—Paragraph A4—Interpretive Note to R1.
[74]POC (MLP) Regulation 7 Section (5A).
[75]Regulation 5B of the Proceeds of Crime (Money Laundering Prevention) Regulations and Regulation 6A (5B) of the Terrorism Prevention (Reporting Entities) Regulations.

2.8.1.5. Written approval for the application of simplified due diligence will not be granted by the Competent Authority unless it is satisfied that the operator has complied with the requirements in paragraph 2.8.1.4 above.

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

- 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
- the operator shall make an assessment as to whether any disclosure is required under section 94 of the POCA (disclosure as to transactions that constitute or are related to money laundering).[76]

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

- requiring only one form of Government-issued identification from the applicant for business concerned, or accepting forms of identification other than Government-issued identification;
- 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;
- 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;
- reliance on publicly available documents or such other documents as the Competent Authority may specify; or
- such other procedures as the Competent Authority may specify.[77]

2.8.1.8. Simplified due diligence will not be permitted if:

- a proper evaluation of the risk has not been conducted by the casino operator, which justifies the adoption of the simplified due diligence procedures;
- there is a suspicion of money laundering, terrorism financing or proliferation financing;
- casino operators have determined that the business relationship or transaction poses a high risk;
- appropriate controls and systems have not been implemented to reduce or mitigate identified risks.

2.8.1.9. A casino operator must discontinue applying simplified due diligence measures, if:

- it doubts the veracity or accuracy of any documents or information previously obtained for the purposes of identification or verification;
- 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
- it suspects money laundering, terrorism financing or proliferation financing.

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

2.8.2. *Enhanced Requirements*

2.8.2.9. 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.

2.8.2.10. 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/CPF 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:

- 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
- 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 CGC and the regulatory/supervisory authorities in that jurisdiction.

2.8.2.11. Under the POC (MLP) Regulations and TP (RE) Regulations, relationships or transactions that are identified as high-risk include:

- politically exposed persons (PEPs);

---

[76]Regulation 7B, POC (MLP) Regulations.

[77]Regulation 7A (5C) of the POC (MLP) Regulations and Regulation 6A (5D) of the TP (RE) Regulations.

- a person who is not ordinarily resident in Jamaica;
- a person acting as a trustee for another in relation to the business relationship or one-off transaction concerned;
- Such other class or category of persons specified by the supervisory authority by notice published in the *Gazette*.

2.8.2.12. The list of relationships or transactions reflected in the POC (MLP) Regulations and TP (RE) Regulations is not exhaustive and can be expanded by the supervisory authority under the POCA, by notice published in the *Gazette*. As such, casino operators are subject to the statutory mandate to establish a risk profile regarding all respective business relationships and one-off transactions. [78] 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.

2.8.2.13. Additional circumstances which, based on the foregoing, appear to increase the risks to a casino operator doing business include:

- verification of identification post commencement of the business relationship;
- customers using cash-only transactions;
- high net worth customers;
- non-face-to-face customers;
- transactions by emerging technology;
- custor rs from countries with inadequate frameworks with respect to AML/CFT/CPF;
- transactions undertaken for occasional customers; or
- wire transfers and other electronic funds transfers.

2.8.2.14. Regulation 7A (4) of the POC (MLP) Regulations and Regulation 6A(4) of the TP (RE) 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:

- obtaining senior management approval to commence or continue the business relationship or one-off transaction;
- examining the background and purpose of the business relationship and transactions, as far as reasonably possible;
- 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;
- 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;
- limiting those business relationships and one-off transactions that appear or have been deemed to be suspicious, in accordance with the appropriate enhanced measures;
- depending on the circumstances of the case:
    - seeking additional independent, reliable sources to verify information provided or made available to the casino operator;
    - taking additional measures to better understand the background and financial situation of the customer;
    - taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship;
    - increasing the monitoring of the business relationship, including greater scrutiny of the transactions; and
    - 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.

2.9. *High Risk Customer*

2.9.1. *Politically Exposed Persons (PEPs)*

2.9.1.1. PEPs are individuals who have been entrusted with prominent public functions and have as a result been deemed high risk. This category of persons includes the following persons and their relatives[79] and close associates:[80]

(a) a head of state or of government;

---

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

[79] Relatives in relation to the person concerned, means spouse, child (including stepchild or adopted child), the spouse of his child, his parents, his brother or sister. See POC (MLP) Regulations, r. 7A(7).

[80] 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 POC (MLP) Regulations, r. 7A(7).

(b) a member of any house of parliament;

(c) a minister of government;

(d) a member of the judiciary;

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

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

(g) a Permanent Secretary, Chief Technical Director or Chief Officer in charge of the operations of a Ministry, department of Government, Executive Agency or Statutory Body;

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

(i) an Official of any political party; or

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

2.9.1.2. 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 POCA, the Competent Authority may direct that businesses in the regulated sector:

- 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);
- provide any reports required at more frequent intervals, as specified in the directions;
- carry out, or permit to be carried out, such additional audit requirements as may be specified in the directions; and
- not rely on any assurance referred to in Regulation 12 of the POC (MLP) Regulations for the purposes of verifying the identity of the person or applicant or business.[81]

2.9.2. *Other High-Risk Customers*

Other High-Risk Customers include:

- a person who is not ordinarily resident in Jamaica;
- a person acting as a trustee for another in relation to the business relationship or one-off transaction concerned;
- a member of such other class or category of persons as the Supervisory Authority may specify by notice published in the *Gazette*;
- a business relationship or transaction with a customer that resides or is domiciled in a specified territory[82] or a country that has been identified as high-risk.

2.9.3. *Additional Considerations*

2.9.3.1. Given the risk assessment profile requirements under the AML/CFT/CPF regulations, as well as the risk-based approach contemplated by the FATF Recommendations, a casino operator would not be precluded from extending the enhanced or heightened measures to persons who are not expressly reflected in the list at regulation 7A(6) of the POC(MLP) Regulations and at regulation 6A(6) of the TP(RE) 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 casino operator's own risk assessment where the profile of the person warrants such an approach being taken. It is expected that in such cases, such a profile would be reflective of the following:

- whether the individual is an elected representative or not:
    - 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
    - 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);
- the individual's prominence or position (as a prominent public figure):
    - facilitates the ability to influence or control (directly or indirectly) the access to and/or use of public property (including funds or benefits); or
    - 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 (i) or (ii) above.

[81]Regulation 7B of the POC (MLP) Regulations.
[82]Section 94A of the POCA.

2.9.3.2. A person who qualifies 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.[83]

2.9.3.3. A casino operator should not establish business relationships with PEPs if the operator 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 operations of the business 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.

2.9.3.4. To mitigate the significant legal and reputational risk that casino operators may face from establishing and maintaining business relationships with PEPs who use funds which were derived from corruption or misuse of public assets, the following procedures should be followed prior to the commencement of such relationships:

- Information gathering forms/procedures should reasonably allow the casino 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 casino operator should also access publicly available information to assist in the determination and confirmation of whether or not an individual is a PEP;
- 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;
- 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;
- 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.

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

- regular reviews of customer identification records to ensure they are kept current; and[84]
- ongoing monitoring of PEP accounts.

2.9.3.6. In the exercise of enhanced due diligence, businesses shall pay particular attention to:

- requests from foreign persons to establish accounts with a casino operator that is unaccustomed to maintaining accounts for overseas customers and which has not sought out such business;
- requests for secrecy in relation to a transaction e.g., booking transaction in the name of a company whose beneficial owner is not disclosed or readily apparent;
- routing of transactions into or through a secrecy jurisdiction;
- deposits or withdrawals of multiple monetary instruments just below reporting threshold on or around same day;
- patterns, where, after deposit or wire transfer is received, there is minimal play, funds from cash-out are shortly thereafter wired to another counterparty/customer (particularly off-shore or secrecy jurisdiction);
- 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; and
- enquiry by or on behalf of a PEP.

2.9.4. *Non-Face-To-Face Customers*

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

2.9.5. *Transactions Undertaken for Occasional Customers*

An occasional customer (e.g. a non-account holder), falls within the definition of 'applicant for business' under the AML/CFT/CPF 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.[85] 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.[86] Where a casino 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 casino operator for a minimum period of seven (7) years.[87]

---

[83] FATF Guidance on Politically Exposed Persons (R12 and 22) June 2013, "B" Time Limits of PEPs Status, paragraph 44, page 12.
[84] POCA (MLP) Regulations, 2007 r. 7(l)(c).
[85] POC (MLP) Regulations, 2007 r,2; TP (Reporting Entities) Regulations, 2010 r.2
[86] POC (MLP) Regulations, 2007 r.6 (l)(a); FATF (Revised) Recommendations r. 10(d). Note that the FATF recommendations (RIO) reflect that CDD for occasional transactions should be applied for transactions above approved threshold limit where there is no suspicion of ML. Jamaica's requirements are therefore more stringent, in this regard as no applicable threshold applies in relation to occasional transactions.
[87] POC (MLP) Regulations, r.14(5).

2.9.6. *Emerging Technology*[88]

2.9.6.1. Casino operators should proactively assess the various risks posed by emerging technologies in the use of new payment products and services[89], and design customer identification procedures with due regard to such risks.

2.9.6.2. New payment products and services (NPPS) are described in the related FATF Guidance[90] 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.

2.9.6.3. 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 of a means of payment. Those providers should be subject to AML/CFT/CPF preventive measures including CDD, record-keeping and reporting of suspicious transactions.

2.9.6.4. Further considerations raised by FATF are that the provision of NPPS:

- usually requires a complex infrastructure involving several parties for the execution of payments. This raises a particular concern when it is not, or cannot be clearly established which of the entities involved is subject to AML/ CFT/CPF obligations and which country is responsible for regulating compliance with those obligations;
- sometimes involves 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/CPF requirements; and
- often involves entities from sectors such as Mobile Network Operators which are unfamiliar with AML/ CFT/CPF 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.

2.9.6.5. 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. Additionally, 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/CPF 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.

2.9.6.6. Using a risk-based approach presumes that based on the risk assessments conducted, a casino operator would not be precluded from providing relaxed measures for NPPS. This occurs if the risk assessment confirms that the profile of the product or service or mechanism warrants such an approach being 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 businesses seek to establish their CDD processes and procedures and prior to the launch of such services, products or mechanisms. This means looking at the ML/TF/PF risks with these the products to minimize vulnerabilities.

2.9.6.7. Casino operators should also bear in mind that Jamaica has legislation in place treating with cybercrimes and lotto scamming activities and should be cognizant of the obligations and offences described in these legislations, as well as those in the Evidence Act and the Electronic Transactions Act.

2.10. *Record Keeping*

2.10.1. *General Legal and Regulatory Requirements*

2.10.1.1. This part of the Guidelines provides guidance on appropriate record-keeping procedures required by the POC(MLP) Regulations and TP(RE) Regulations.

2.10.1.2. The purpose of the record-keeping requirements is to ensure that there is an audit trail that could assist in any investigation by a law enforcement body. These records are also important when the CGC is conducting an investigation for compliance purposes.

2.10.1.3. The operator's record-keeping policy and procedure should cover records in the following areas:

- details of how compliance has been monitored by the Nominated Officer;
- delegation of AML/CFT tasks by the Nominated Officer;
- Nominated Officer reports to senior management;
- information not acted upon by the Nominated Officer, with reasoning as to why no further action was taken;

[88]FATF Recommendation 15.
[89]Regulation 6(iv) of the Amendments to POC (MLP) Regulations.
[90]FATF Guidance on Prepaid Cards, Mobile Payments and Internet-Based Payment Services, June 2013.

- customer identification and verification information;
- supporting records in respect of business relationships or occasional transactions;
- employee training records;
- internal and external STRs; and
- contact between the Nominated Officer and law enforcement or FID, including records connected to appropriate consent.

2.10.1.4. The policy and procedure for record-keeping should also make provision for the retrieval and retention by the casino operator of records formerly held by an employee who leaves the business.

2.10.1.5. The record-keeping requirements for supporting records, that is, the records of ongoing transactions with a customer, are based on the nature of the relationship with that customer. There may be:

- no relationship;
- a 'business relationship', depending on the circumstances; or
- an 'occasional transaction'.

2.10.2. *Business relationships*

2.10.2.1. A business relationship is a business, professional or commercial relationship between a casino operator and a customer which arises out of the business of the casino operator and the casino expects their relationship to have an element of duration. Casino operators are encouraged to interpret this definition widely.

2.10.2.2. Casinos are likely to form a business relationship when:

- the casino starts tracking a customer's drop/win figures;
- a customer opens an account with the operator or joins a membership scheme; or
- a customer obtains a cheque cashing facility.

2.10.2.3. 'Ongoing monitoring of business relationships' is a requirement for casino operators and includes scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile.[91]

2.10.2.4. Casinos are expected to approach this requirement on a risk basis. Dependent on how frequently a casino forms 'business relationships' it may be good practice to apply ongoing monitoring more widely. Regular players should be the subject of closer scrutiny and their level of play should be assessed with reference to the information already known about them, and where necessary, additional information must be collected and retained about the source of their funds.

2.10.3. *One-off Transactions/Occasional Transactions*

A casino may undertake a one-off transaction with a customer when there is no business relationship but the customer purchases or exchanges chips over the approved threshold limit in value. For example, a customer on a single visit to a casino while on holiday or a business trip who purchases or exchanges chips over the approved threshold limit constitutes a 'one-off transaction'. CDD will need to be done under these circumstances and the casino will have to retain the supporting records, that is, the drop/win data, for seven (7) years after the date of the visit.

2.10.4. *Other Casino Customers*

Some casino customers may not fall into the business relationship or one-off transaction definitions. For example, customers spending low amounts at gaming during single, infrequent and irregular visits to a casino and who are not subject to tracking. There may be no expectation at any stage that there will be any duration to the relationship with the customer. Strictly speaking such business falls outside of the record-keeping requirements.

2.10.5. *Customer information*

In relation to the evidence of a customer's identity, operators must keep a copy of, or the references to, the verification evidence of the customer's identity obtained during the application of CDD measures.

2.10.6. An operator may often hold additional information beyond identity in respect of a customer for the purposes of wider customer due diligence. As a matter of best practice this information and any relevant documents should also be retained.

2.10.7. There is a separate requirement in the POC (MLP) Regulations to ensure that documents, data or information held by casinos are kept up to date.[92] A trigger event for refreshing and extending CDD may occur where a customer returns to a casino after a period of non-attendance. Refreshing information about existing customers will ensure that matters such as change of address, or a customer being appointed into a role which attracts PEP status, will be picked up. Keeping information up to date is also a requirement under the POCA and the Casino Gaming Act. How these issues will be dealt with in practice should be covered in the casino's policies and procedures.

[91]POC (MLP) Regulation 7A.
[92]POC (MLP) Regulation 7A(5).

2.10.8. *Supporting records*

2.10.8.1. The requirement to keep supporting records is linked to, business relationships' and 'one-off transactions' (which are defined in the POC (MLP) Regulations[93]) and the extent and nature of records created. In many casinos, customers (regardless of whether or not they have formed a business relationship or are part of an one-off transaction) purchase chips with cash at the gaming tables where, in low risk situations, no records are created and therefore not available to be kept.

2.10.8.2. The CGC expects casino operators to use reasonable endeavours to keep supporting records and to make it clear in their policies, procedures and controls what records will be created in light of the known spending patterns and the assessed money laundering and terrorist financing risks at each premises.

2.10.8.3. Some casinos undertake a process at the end of each business day to count the total drop (cash used to purchase chips) to compare against the total amount recorded through tracking individual customer spending. The difference between the two (2) figures is the amount of drop that is not attributable to particular customers. This in turn can be calculated against known attendance figures and the number of customers tracked to give an average amount of money used to purchase chips per customer that has not been tracked, and therefore has no supporting records. Where this process is used, it should be the subject of ongoing risk assessment for each premises and the records created during the process should also be retained.

2.10.8.4. Any casino operator devising its record-keeping policy and procedure should decide how a customer fits within the definitions of 'business relationship' or 'one-off transaction'. The variation in the record-keeping requirements for different circumstances illustrates the flexibility available to casinos which allows them to focus their resources on higher money laundering risk situations.

2.10.8.5. For the purposes of supporting records, the CGC takes the view that in most cases this will consist of records covering the drop/win figures, subject to paragraph 2.10.4 of these Guidelines, for each customer for each 24 hour period. There is no requirement to keep detailed records for each customer for each table or game for AML purposes. However, the CGC may require operators to maintain records for each table or game but not broken down by each customer's transactions.

2.10.9. *Supporting records - gaming machines*

2.10.9.1. Cash-in with cash-out gaming machines do not produce any supporting records that can be attributed to a customer. They do generate overall cash-in and cash-out data that must be retained by the casino. However, 'ticket in, ticket out' (TITO) and 'smart card' technology may mean that, in the future, machines produce supporting records that can be attributed to a customer who falls within the record keeping requirements, in which case such records must be retained in accordance with the Regulations.

2.10.9.2. The essentials of any system of monitoring are that:

- it flags up transactions and/or activities for further examination;
- these reports are reviewed promptly by the Nominated Officer; and
- appropriate action is taken on the findings of any further examination.

2.10.9.3. Monitoring can be either:

- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place; or
- after the event, through the Nominated Officer's review of the transactions and/or activities that a customer has undertaken.

2.10.9.4. In either case, unusual transactions or activities should be flagged for further examination.

2.10.9.5. In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer risk.

2.10.9.6. Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the operator's business activities, and whether the operator is large or small. The key elements of any system are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.

2.10.10. *Retention period*[94]

2.10.10.1. Records of identification and verification of customers must be kept for a period of at least seven (7) years[95] after the business relationship or one-off transaction with the customer has ended. The date the relationship with the customer ends is the last date on which they visit or use a casino.

2.10.10.2. Supporting records must be retained for a period of seven (7) years, beginning on the date any transaction is completed where the records relate to a particular transaction. This creates a rolling seven (7) years history of drop/ win data. Records of internal and external reports on suspicious activity should be retained for seven (7) years from when the report was made.

2.10.11. Form in which records have to be kept

---

[93]POC (MLP) Regulation 2.
[94]POCA section 94(4).
[95]POCA (MLP) Regulations, r. 14(5)(a).

2.10.11.1. Most operators have record-keeping procedures which they keep under review, and will seek to reduce the volume and density of records which have to be stored, whilst still complying with statutory requirements. Retention may therefore be:

- by way of original documents;
- by way of photocopies of original documents;
- on microfiche;
- in scanned form; or
- in computerised or electronic form.

2.10.11.2. Records relating to ongoing investigations should, where possible, be retained until the relevant law enforcement agency has confirmed that the case has been concluded.

2.10.11.3. Where the record-keeping obligations under the POC (MLP) Regulations and TP (RE) are not observed, an operator or person is open to prosecution and sanctions, including imprisonment and/or a fine, or regulatory censure.

2.11. *Suspicious Activities and Reporting*

2.11.1. *Introduction*

2.11.1.1. Section 94 of the POCA 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:

- that a person 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 (Section 94(2)(a));
- the information or matter on which the knowledge or belief is based, or which gives reasonable grounds for such knowledge or belief, was obtained in the course of a business in the regulated sector (section 94(2)(b)); and
- the person must make the required disclosure as soon as is reasonably practicable, and in any event within fifteen (15) days, after the information or other matter comes to him.

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

- 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
- 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.

2.11.1.3. In complying with the obligation to report suspicious transactions under the POCA and the TPA, a casino operator is also required to:

- pay attention to (or identify and take notice of):
- complex, unusual or large business transactions, or unusually large transactions carried out by the customer with the casino operator;
- unusual patterns of transactions;
- unusual employment of an intermediary in the course of some usual transaction or financial activity;
- unusual method of settlement;
- make a record of these transactions and the related findings;[96]
- 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;
- 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.

2.11.1.4. Where a casino operator knows or believes, or has reasonable grounds for knowing or believing, that a customer or prospective customer is engaging in ML activities/transactions, he must either:

(a) refuse—

(i) to conduct the transaction;

(ii) 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

[96]Section 94(4)(a) POCA; section 16(2) TPA.

(b) seek appropriate consent, through the Nominated Officer, from the Designated Authority to proceed with the transaction.[97]

2.11.1.5. Severe implications such as prosecution and/or reputational damage can arise when a casino operator holds property or provides services to facilitate ML/TF/PF. The regulated business shall ensure that such accounts or transactions are subject to appropriate counter measures to safeguard the business. Counter measures include action to:

- close the account;
- end the business relationship;
- terminate the transaction;
- scale down gaming services;
- refuse to undertake transactions above a certain amount;
- refuse to undertake new business with the customer.

2.11.1.5.1. The application of appropriate counter measures by a casino 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 a regulated business 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. Casino operators must be in a position to make their findings in this regard available to the CGC, upon request. These findings must also be available to the Designated Authority.

2.11.1.6. Casino operators should also note the following:

(a) if the regulated business has a reasonable excuse for failing to make the disclosure before proceeding with the transaction, relationship or arrangement, then the regulated business must ensure that the relevant disclosure is made on its own initiative and as soon as is reasonably practical;[98]

(b) further to (a) the business 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.

2.11.1.7. Casino 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.

2.11.1.8. Casino 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.

2.11.1.9. 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:

- identifying and taking notice of the types of transactions described in these sections of the law;
- the examination of the background and purpose of these types of transactions;
- the formal recording of the findings of the business; and
- the retention of the findings of the business for a period not less than seven (7) years.

2.11.2. *Protected and Authorized Disclosures*

2.11.2.1. Under section 100 of the POCA, a disclosure is protected if it satisfies the following conditions and does not breach any disclosure restraints, however imposed:

- the information or other matter disclosed was obtained in the course of the reporting person's trade, profession, business or employment;
- 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
- the disclosure is made to an authorized officer[99] or Nominated Officer as soon as is reasonably practicable after the said information or other matter comes to the person making the disclosure.

2.11.2.2. An authorized disclosure is described in subsection 100 (4) of the POCA as follows—

(a) it is a disclosure to an authorized officer or Nominated Officer that property is criminal property;

(b) it is made in such form and manner as may be prescribed by regulations made under section 102, and

(c) either of the following, (i) or (ii), is satisfied—

(i) the disclosure is made before the person making the disclosure does the prohibited act; or

(ii) all of the following—

A. the disclosure is made after the person making the disclosure does the prohibited act;

[97]See POCA sections 93(2); 99 and 100(4) and (5).
[98]POCA Section 100(4) and (5).
[99]In this section, an authorized officer is an officer of the FID, a constable or a customs officer.

B. the person has a reasonable excuse for failing to make the disclosure before doing the act; and

C. the disclosure is made on the person's own initiative and as soon as it is reasonably practicable for him to make it.

2.11.2.3. 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 of the POCA) to conduct the prohibited act.

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

2.11.2.5. 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.[100]

2.11.2.6. Employees in casinos are required to make a report in respect of information that comes to them within the course of their business:

- where they know; or
- where they suspect; or
- where they have reasonable grounds for knowing or suspecting,
- that a person is engaged in money laundering or terrorist financing. Within this guidance, the above obligations are collectively referred to as 'grounds for knowledge or suspicion'.[101]

2.11.2.7. In order to provide a framework within which reports of suspicion may be raised and considered:

- each operator must ensure that any employee reports to the operator's Nominated Officer where they have grounds for knowledge or suspicion that a person or customer is engaged in money laundering or terrorist financing;
- the operator's Nominated Officer must consider each such report, and determine whether it gives grounds for knowledge or suspicion;
- operators should ensure that employees are appropriately trained in their obligations, and in the requirements for making reports to their Nominated Officer.

2.11.2.8. Casino 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 casino 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.

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

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

- be sufficiently detailed, clear and precise;
- set out the rationale for suspicion;
- indicate the particular unusual nature of the transaction;
- provide contrasting historical data; and
- set out the chronology of events.

2.11.3. *What is meant by knowledge and suspicion*?

2.11.3.1. Having knowledge means actually knowing something to be true. In a criminal court, it must be proved that the individual in fact knew that a person was engaged in money laundering. That said, knowledge can be inferred from the surrounding circumstances, so, for example, a failure to ask obvious questions may be relied upon by a jury to infer knowledge. The knowledge must, however, have come to the operator (or to the employee) in the course of casino business or (in the case of a Nominated Officer) as a consequence of a disclosure under section 91 of POCA. Information that comes to the operator or employee in other circumstances does not come within the scope of the regulated sector's obligation to make a report. This does not preclude a report being made should employees choose to do so.

2.11.3.2. Employees may also be obliged to make a report by other parts of the POCA.

---

[100]This form is available on the FID's website at www.fid.gov.jm.
[101]Section 94(2).

2.11.3.3. In the UK case of *Da Silva* [2006] EWCA Crim 1654, the Court of Appeal stated the following in relation to suspicion:

'It seems to us that the essential element in the word "suspect" and its affiliates, in this context, is that the defendant must think that there is a possibility, which is more than fanciful, that the relevant facts exist. A vague feeling of unease would not suffice.'

2.11.3.4. There is thus no requirement for the suspicion to be clear or firmly grounded on specific facts, but there must be a degree of satisfaction, not necessarily amounting to belief but at least extending beyond mere speculation, that an event has occurred or not.

2.11.3.5. Whether you hold suspicion or not is a subjective test. If you think a transaction is suspicious you are not expected to know the exact nature of the criminal offence or that particular funds are definitely those arising from the crime. You may have noticed something unusual or unexpected and, after making enquiries, the facts do not seem normal or make commercial sense. You do not need to have evidence that money laundering is taking place to have suspicion.

2.11.3.6. 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:

- general knowledge of the nature of the industry/sector in which the customer operates;
- the nature and pattern of the customer's own business;
- a good understanding of the operating environment; and
- the financial processes that would be applicable to the various services and products offered.

2.11.3.7. Unusual patterns of gambling, including the spending of particularly large amounts of money in relation to the casino or customer's profile, should receive attention, but unusual behaviour should not necessarily lead to grounds for knowledge or suspicion of money laundering, or the making of a report to FID. The Nominated Officer is required to assess all of the circumstances and, in some cases, it may be helpful to ask the customer or others more questions. The choice depends on what is already known about the customer and the transaction, and how easy it is to make enquiries.

2.11.3.8. In order for either an internal or external report to be made it is not necessary to know or to establish the exact nature of any underlying criminal offence, or that the particular funds or property were definitely those arising from a crime.

2.11.4. What is meant by reasonable grounds to know or suspect?

2.11.4.1. In addition to establishing a criminal offence relating to suspicion or actual knowledge of money laundering, POCA creates criminal liability for failing to disclose information when reasonable grounds exist for knowing or suspecting that a person is engaged in money laundering[102] or terrorist financing. This lower test, which introduces an objective test of suspicion, applies to all businesses covered by the Regulations, including casinos. The test would likely be met when there are demonstrated to be facts or circumstances, known to the employee in the course of business, from which a reasonable person engaged in a casino business would have inferred knowledge, or formed a suspicion, that another person was engaged in money laundering or terrorist financing.

2.11.4.2. To defend themselves against a charge that they failed to make a report when the objective test of suspicion has been satisfied, employees within casinos would need to be able to demonstrate that they took reasonable steps in the particular circumstances (and in the context of a risk-based approach) to conduct the appropriate level of CDD. It is important to bear in mind that, in practice, a court will be deciding, with the benefit of hindsight, whether the objective test was met.

2.11.5. *Internal reporting*

2.11.5.1. Employees of a casino operator obtain a legal defence if they report to the Nominated Officer where they have grounds for knowledge or suspicion. All casino operators therefore need to ensure that all relevant employees know they should report suspicions to their Nominated Officer. Internal reports to a Nominated officer, and reports made by a Nominated Officer to FID, must be made within fifteen (15) days in each case. 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.

2.11.5.2. All suspicions reported to the Nominated Officer should be documented or electronically recorded. The report should include full details of the customer who is the subject of concern and as full a statement as possible of the information giving rise to the grounds for knowledge or suspicion. All internal enquiries made in relation to the report should also be documented or electronically recorded. This information may be required to supplement the initial report or as evidence of good practice and best endeavours if, at some future date, there is an investigation.

2.11.5.3. Once an employee has reported his suspicion to the Nominated Officer, or to an individual to whom the Nominated Officer has delegated the responsibility to receive such internal reports, he has fully satisfied his statutory obligation.[103]

2.11.6. *Evaluation and Determination by the Nominated Officer*

2.11.6.1. The operator's Nominated Officer must consider each report and determine whether it gives rise to grounds for knowledge or suspicion. The operator must permit the Nominated Officer to have access to any information, including CDD information, in the operator's possession that could be relevant. The Nominated Officer may also require further information to be obtained from the customer, if necessary.

[102]Section 94 POCA.
[103]Section 94(4) POCA.

2.11.6.2. Any approach to the customer should be made sensitively and probably by someone already known to the customer, to minimize the risk of alerting the customer or an intermediary that a disclosure to FID is being considered.

2.11.6.3. If the Nominated Officer decides not to make a report to FID, the reasons for not doing so should be clearly documented or electronically recorded, and retained. These records should be kept separately by the Nominated Officer in order that the information therein is not disclosed accidentally.

2.11.7. *External reporting*

2.11.7.1. To avoid committing a failure to report offence, the Nominated Officer must make a disclosure to FID where he decides that a report gives rise to grounds for knowledge or suspicion.

2.11.7.2. The Nominated Officer must report to FID any transaction or activity that, after his evaluation, he knows or suspects, or has reasonable grounds to know or suspect, may be linked to money laundering. Such reports must be made as soon as is reasonably practicable after the information comes to the Nominated Officer and in any event within fifteen (15) days after the information or other matter came to the Nominated Officer.[104]

2.11.8. *Submission of suspicious activity reports*

2.11.8.1. FID accepts the submission of STRs in two (2) ways:

(a) Paper based reporting by way of Form 1 - Suspicious Transaction Report. The form is available for download from the FID website (www.fid.gov.jm). Reports must be sent in sealed envelopes/ packages stamped "Confidential" and addressed to: The Designated Authority, The Chief Technical Director, Financial Investigations Division, Ministry of Finance & Planning, 1 Shalimar Avenue, Kingston 3. It is very important that Reporting Entities ensure that packages and letters sent to the Designated Authority are pr verly addressed. Failure to do so may result in unauthorized disclosures.

(b) Online Reporting r. 17 of POC (MLP) Regulations, allows the Designated Authority (FID) to amend Form 1 and also to allow for this form to be submitted in an electronic format. When implemented, online reporting will be mandatory.

2.11.8.2. Operators should include in each STR as much relevant information about the customer, transaction or activity that it has in its records. At a minimum, the STR must have the following information:

- Reporting Casino Operator
- Name & Telephone number for Nominated Officer (or his designate)
- Full Name of Customer
- TRN (or other national registration number) of Customer
- Address of Customer
- Date of Birth of Customer
- Identification Information
- Name of person conducting transaction (Agent)
- Transaction type
- Transaction date/period
- Transaction currency
- Transaction Amount
- Jamaican Dollar Equivalent
- US Dollar Equivalent
- Reasons for suspicion (for STR)

2.11.7.3. In order that an informed overview of the situation may be maintained, all contact between operators and law enforcement agencies should be controlled through, or reported back to, the Nominated Officer or a deputy acting in the absence of the Nominated Officer.

2.11.8. *Appropriate consent*

2.11.8.1. If operators handle any proceeds of crime they may commit one of the principal money laundering offences in POCA or the TPA. However, if the Nominated Officer makes a report to FID this can amount to a defence. The 'reporting defence' includes the statutory mechanism which allows FID either to agree to the transaction going ahead, or to prevent the suspected money laundering going ahead. This statutory mechanism is called 'appropriate consent.'[105]

2.11.8.2. Under section 91 (2) of the POCA appropriate consent occurs:

- when the Nominated Officer receives consent from the Designated Authority within seven (7) business days of the Nominated Officer's disclosure and request for consent to undertake the prohibited transaction;[106]
- 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 (7) business days; or[107]
- after the Nominated Officer makes a disclosure to the Designated Authority, and that Officer has received notification from the Designated Authority within the seven (7) business days denying consent, but ten (10) days have passed since the receipt of that notice.[108]

---

[104]Section 94(2) POCA.
[105]Sections 91(2)(a) and (b), 91(3) and 99, POCA.
[106]Sections 99(l)(a), POCA
[107]Sections 91(2)(b)(i) and 99(l)(b), POCA.
[108]Sections 91(2)(b)(ii) and 99(1)(c), POCA.

2.11.8.3. Where a casino operator has knowledge or reasonable grounds to believe that the funds involved in a transaction are criminal property, the operator must obtain the appropriate consent from FID before doing that transaction or otherwise decline to proceed with the transaction. Failing this, the regulated business may be liable for engaging in a prohibited act. A prohibited act is defined as a money laundering offence under sections 92 and 93 of POCA.

2.11.8.4. Consent should be requested through the completion and submission to the FID of an Authorized Disclosure (Form III). The form is available at the FID website (www.fid.gov.jm).

2.11.9. Proceeding with Transactions after Consent has been Requested

2.11.9.1. The Nominated Officer may give the appropriate consent to the doing of a prohibited act in instances where the Nominated Officer has made a disclosure to the FID indicating that property is suspected criminal property and any of the following occurs:

- FID gives consent to the transaction;
- Having made the report, seven (7) working days have passed and the Nominated Officer has not received a response from the FID; or
- The Nominated Officer receives a response before the seven (7) working days have elapsed that consent was refused, but ten (10) days have passed since the receipt of that refusal notice without any subsequent judicial action.

2.11.9.2. Where an urgent response to a consent request is required, the FID is permitted to provide a verbal notice of his consent or refusal. The casino operator must still submit an authorized disclosure (Form III) to the FID but this can be sent by electronic mail. A written notice (confirmation) shall be sent by the FID within five (5) days of that verbal response to the Nominated Officer.

2.11.10. *Future Requests for Consent for the same Customer*

2.11.10.1. Where the customer continues to conduct other similar transactions that are believed to involve criminal property, the regulated business is required to seek consent for each prohibited act. However, it is not necessary to seek the consent of the FID to conduct another type of transaction with that customer where the funds involved appear to be from a legitimate source.

2.11.10.2. The FID will not provide a general "blanket" consent to the conduct of all future transactions with a particular customer. The requirement for consent is in relation to a particular activity or transaction.

2.11.11. *Communicating with Customers during the Consent Period*

2.11.11.1. In corresponding with the customer, the regulated business must be conscious of the tipping-off provisions and unauthorized disclosures under POCA. Therefore, the regulated business cannot tell the customer:

- during the notice period (seven (7) working days), that the transaction is being delayed because it is awaiting consent from the Designated Authority;
- during the ten (10) day moratorium period, that consent was refused by the Designated Authority;
- At a later date, that the transaction was delayed because the consent of the Designated Authority was being sought; or
- that law enforcement is conducting an investigation.

2.11.11.2. A regulated business can tell its customers that it is carrying out its required due diligence checks and procedures to comply with all applicable laws and its own internal procedures. It may be useful for regulated businesses to make customers aware in their contracts that transactions may sometimes be delayed or refused because of their obligations under the governing statutes. This would provide an explanation for the delay in processing a transaction without violating the tipping-off provisions.

2.11.11.3. A report made after moneylaundering has already taken place will only be a legal defence if there was a 'reasonable excuse' for failing to make the report before the money laundering took place.[109]

Where a customer's instruction is received prior to a transaction or activity taking place, or arrangements being put in place, and there are grounds for knowledge or suspicion that the transaction, arrangements, or the funds/property involved, may relate to money laundering, a report must be made to FID and consent sought to proceed with that transaction or activity. In such circumstances, it is an offence for a Nominated Officer to consent to a transaction or activity going ahead within the seven (7) working day, notice period from the working day following the date of disclosure, unless FID gives consent.

2.11.11.4. In the casino environment, business is often conducted out of normal office hours and in circumstances where it is not feasible to obtain appropriate consent prior to or during a transaction. Grounds for knowledge or suspicion may be triggered after a customer has completed the three (3) stages of a gambling transaction; that is, they have bought in, they have played and they have cashed out. Under these circumstances, it would be reasonable to report after the transaction. However, the defence of 'reasonable excuse' when reporting after the transaction is untested by case law, and would need to be considered on a case-by-case basis.

2.11.11.5. Casinos should include in their policies and procedures details on how they will manage circumstances where there are grounds for knowledge or suspicion of money laundering or terrorist financing. If knowledge or suspicion is present then there must be a mechanism for involvement of the senior manager on duty and contact with the

[109]Section 94(6) POCA.

Nominated Officer as soon as is practicable. If the circumstances amount to reasonable grounds to suspect, then reporting the matter to the Nominated Officer should be sufficient, and for the Nominated Officer to receive the matter at the earliest practicable opportunity.

2.11.11.6. The Nominated Officer will need to think very carefully about whether or not he wishes to continue to do business with the suspected customer. Relevant considerations should be the potential commission of criminal offences under the POCA or the TPA, as well as potential damage to reputation and other commercial factors.

2.11.11.7. Operators should also note that in the CGC's view the reporting defence is not intended to be used repeatedly in relation to the same customer. If patterns of gambling lead to a steadily increasing level of suspicion of money laundering, or even to actual knowledge of money laundering, operators will no doubt seriously consider whether they wish to allow the customer to continue using their gaming facilities. Operators are of course free to terminate their business relationships if they wish, and provided this is handled sensitively there will be no risk of 'tipping-off' However, if the decision has been made to terminate gaming facilities and there is a remaining suspicion of money laundering/terrorist financing with funds to repatriate, consideration should be given to asking for appropriate consent.

2.11.11.8. How customers suspected of money laundering will be dealt with is an important area of risk management for all operators. Casinos should deal with the issue in their policies and procedures and, as all gambling operators are at risk of committing the principal offences, it is advisable for operators to consider these issues carefully before they arise in practice.

2.11.11.9. Although one transaction may be suspicious and be reported as such, there may be less concern that all of an individual's future transactions will be suspicious. In these circumstances, each transaction should be considered on a case-by-case basis and reports made accordingly. Where subsequent reports are also made after actual or suspected money laundering has taken place or appears to have taken place, the Nominated Officer is encouraged to keep records about why reporting was delayed, and about why appropriate consent was not requested before the suspected money laundering took place.

2.11.12. *Tipping off, or prejudicing an investigation*

2.11.12.1. Under section 97(1) of POCA a person commits an offence if:

- knowing or having reasonable grounds to believe that a disclosure falling within section 100 has been made, or is to be made, the person discloses to another person any information, or any other matter, relating to the first mentioned disclosure;
- the person knowing or having reasonable grounds to believe that the Agency, the Director of Public Prosecutions, or an authorized officer as defined by section 103 is acting or proposing to act in connection with a money laundering investigation which is being, or about to be, conducted, he discloses information or any other matter relating to the investigation to any other person.

2.11.12.2. A person does not commit an offence under the section if—

(a) the disclosure is made in carrying out a function that the person has relating to the enforcement of any provision of the Act or any other enactment relating to criminal conduct or benefit from criminal conduct;

(b) the disclosure is to an attorney-at-law for the purpose of obtaining legal advice;

(c) the person is an attorney-at-law and the disclosure falls within an exception specified in subsection (3) of that section; or

(d) the disclosure is a disclosure to the Competent Authority.

2.11.12.3. 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 casino operator that an offence is being attempted or has been or is being committed.

2.11.12.4. Operators should ensure that they have the ability to legally terminate arrangements, transactions or the business relationship, where the casino operator forms 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 business due to the suspected criminal activity.

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

2.11.12.6. Under sections 104 (1) and (2) of POCA where a person knows or has reasonable grounds to believe that an appropriate officer[110] is acting, or proposing to act, in connection with a forfeiture investigation, a civil recovery investigation or a money laundering investigation that is being or is about to be conducted, that person in the regulated sector commits an offence if he:

(a) makes a disclosure that is likely to prejudice the investigation; or

(b) falsifies, conceals, destroys or otherwise disposes of, or causes or permits the falsification, concealment, destruction or disposal of, documents which are relevant to the investigation.

[110]The Nominated Officer or his nominee.

2.11.12.7. A person does not commit the offence of making a disclosure that is likely to prejudice the investigation if:

(a) he does not know or have reasonable grounds to believe that the disclosure is likely to prejudice the investigation;

(b) he does not intend to conceal any facts disclosed by the documents from any appropriate officer carrying out the investigation; or

(c) the person is an attorney-at-law and the disclosure falls within subsection (4).[11]

2.11.12.8. A person does not commit the offence of falsifying, concealing, destroying or otherwise disposing of, or causing or permit the falsification, concealment, destruction or disposal of, documents which are relevant to the investigation if:

(a) he does not know or suspect that the documents are relevant to the investigation; or

(b) he does not intend to conceal any facts disclosed by the documents from any appropriate officer carrying out the investigation.

2.11.12.9. For committing either of the offences mentioned in section 104 (2) of the POCA:

(a) on conviction before a Parish Court Judge, he is liable to a fine not exceeding one million dollars ($1,000,000.00) or to imprisonment for a term not exceeding twelve (12) months or to both such fine and imprisonment; or

(b) on conviction on indictment before a Circuit Court, he is liable to a fine or to imprisonment for a term not exceeding ten (10) years or to both such fine and imprisonment.

2.11.12.10. It is important to note that subsection 104 (7) of the POCA reminds us that, in spite of the prohibitions to disclose, nothing in the section prohibits a disclosure made to the Competent Authority by a business in the regulated sector in respect of a money laundering investigation or any order served upon that business pursuant to that Part of the Act.

2.11.12.11. The POCA therefore, in this regard, contains separate offences of tipping off and prejudicing an investigation. These offences are similar and overlapping, but there are also significant differences between them. It is important for those working in the regulated sector to be aware of the conditions for each offence. Each offence relates to situations where the information on which the disclosure was based came to the person making the disclosure in the course of a business in the regulated sector. The Terrorism Prevention Act contains similar offences.

2.11.12.12. Once an internal or external report of suspicious activity has been made, it is a criminal offence for anyone to release information that is likely to prejudice an investigation that might be conducted following that disclosure. Reasonable enquiries of a customer, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice, forms an integral part of CDD measures and should not give rise to tipping off.

2.11.12.13. Where a confiscation investigation, a civil recovery investigation, a detained cash investigation or a money laundering investigation is being, or is about to be, conducted, it is a criminal offence for anyone to disclose this fact if that disclosure is likely to prejudice the investigation. It is also a criminal offence to falsify, conceal, destroy or otherwise dispose of documents which are relevant to the investigation (or to cause or permit these offences). It is, however, a defence if the person does not know or suspect that disclosure is likely to prejudice the investigation, or if the disclosure is permitted under the POCA or the TPA.

2.11.12.14. An offence is not committed under the POCA or the TPA if the disclosure is made to the relevant supervisory authority (the CGC) for the purpose of:

(a) the detection, investigation or prosecution of a criminal offence in Jamaica or elsewhere;

(b) an investigation under POCA; or

(c) the enforcement of any order of a court under the POCA.

2.11.12.15. An employee, officer or partner of a casino operator does not commit an offence under the POCA or the TPA if the disclosure is to an employee, officer or partner of the operator.

2.11.12.16. A person does not commit an offence under the POCA or the TPA if the person does not know or suspect that the disclosure is likely to prejudice:

(a) any investigation that might be conducted following a disclosure; or

(b) an investigation into allegations that an offence under Part V of the POCA or Section 17 of the TPA has been committed, is being contemplated or is being carried out.

2.11.12.17. The fact that a transaction is notified to FID before the event, and FID does not refuse consent within seven (7) working days following the day after disclosure is made, or a restraint order is not obtained within the moratorium period, does not alter the position so far as 'tipping off' is concerned.

---

[11]Section 104 (4) states that:

"(4) A disclosure falls within this subsection if it is a disclosure—

(a) to, or to a representative of, a client of the attorney-at-law in connection with the giving by the attorney-at-law of legal advice to the client; or

(b) to any person in connection with legal proceedings or contemplated legal proceedings:

Provided that a disclosure does not fall within this subsection if the disclosure is made with the intention of furthering a criminal purpose."

ANTI-MONEY LAUNDERING AND COUNTER TERRORISM FINANCING

Glossary of Terms

• AML	Anti-Money Laundering.
• Business relationship	A business, professional or commercial relationship between a casino operator and a customer, which is expected to have an element of duration.
• Casino	In accordance with the Interpretation Section of the Casino Gaming Act 2010, casino means any premises, part of any premises, or a facility, in or in which casino gaming business is conducted.
• CDD	Customer Due Diligence
• CFT	Combating the Financing of Terrorism
• CGC	Casino Gaming Commission
• Competent Authority	An entity or authority as per POCA Sec 91(g), TPA Sec 18(5) and FIDA Sec 2, authorized by the Minister to monitor compliance and issue guidelines to businesses in the regulated sector. Additional functions may be found in POCA Sec 91A and TPA Sec 18A.
• Criminal spend	In the context of gambling, the use of the proceeds of crime to fund gambling as a leisure activity (also known as "lifestyle spend").
• Customer tracking	The process of capturing drop and win data for a customer.
• Designated Authority (DA)	The Designated Authority, The Chief Technical Director, Financial Investigations Division, Ministry of Finance & the Public Services, 1 Shalimar Avenue, Kingston 3.
• DLT	Distributed Ledger Technology
• DNFBP/DNFI	Designated Non-Financial Businesses and Professions/Designated Non-Financial Institution
• DPRK	Democratic People's Republic of Korea
• Drop/win figures	Data recorded by casinos that covers the total value of chips purchased as well as the total loss or win for a customer over a 24 hour period.
• FID	Financial Investigations Division
• FIDA	Financial Investigations Division Act
• Money laundering	The process by which criminal or 'dirty' money is legitimised or made 'clean', including any action taken to conceal, arrange, use or possess the proceeds of any criminal conduct. Defined in section 91 of POCA.
• Nominated Officer	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) in accordance with the AML/CTF/CPF laws, Guidelines and the conditions of licence of the casino operator, and the reporting of transactions to the FID.
• Operators	Firms holding an operator's licence issued by the CGC.
• POCA	The Proceeds of Crime Act 2007, which is intended to reduce money laundering and the profitability of organised crime through the use of tools such as asset recovery.
• Proceeds of crime	Property from which a person benefits directly or indirectly, by being party to criminal activity, for example, stolen money, money from drug dealing or property stolen in a burglary or robbery.
• SRB	Self-Regulatory Body
• STR	A Suspicious Transaction Report is the means by which suspicious activity relating to possible money laundering or the financing of terrorism is reported to FID under the POCA or the TPA.
• The Regulations	The Proceeds of Crime (Money Laundering Prevention) Regulations made pursuant to the Casino Gaming Act, 2010.
• TPA	Terrorism Prevention Act
• UNSCRIA	United Nations Security Council Resolutions Implementation Act
• UNSC	United Nations Security Council

2.11.12.18. This means that an operator:

(a) cannot, at the time, tell a customer that a transaction is being delayed because a report is awaiting consent from FID;

(b) cannot, later, tell a customer that a transaction or activity was delayed because a report had been made under POCA or the Terrorism Prevention Act, unless law enforcement or FID agrees, or a court order is obtained permitting disclosure; and

(c) cannot tell the customer that law enforcement is conducting an investigation.

2.11.12.19. The judgement in the UK case of *K v Natwest* [2006] EWCA Civ 1039 confirmed the application of these provisions which are similar to the provisions of the UK POCA and terrorism prevention legislation. The judgement in this case also dealt with the issue of suspicion stating that the—

"The existence of suspicion is a subjective fact. There is no legal requirement that there should be reasonable grounds for the suspicion. The relevant bank employee either suspects or he does not. If he does suspect, he must (either himself or through the Bank's Nominated Officer) inform the authorities."

2.11.12.20. The existence of a STR cannot be revealed to any customer of the casino at any time, whether or not consent has been requested. However, there is nothing in POCA which prevents operators from making normal enquiries about customer transactions in order to help remove any concerns about the transaction and enable the operator to decide whether to proceed with the transaction. These enquiries will only constitute tipping off if the operator discloses that a STR has been made to FID or a Nominated Officer, or that a money laundering investigation is being carried out or is being contemplated.

2.11.12.21. The combined effect of these two (2) offences is that one or more of them can be committed before or after a disclosure has been made.

2.11.12.22. The offence of money laundering, and the duty to report under POCA, apply in relation to the proceeds of any criminal activity, wherever conducted, including abroad, that would constitute an offence if it took place in Jamaica. A person does not commit an offence where it is known or believed on reasonable grounds that the conduct occurred outside Jamaica; and the conduct was not criminal in the country where it took place. However, if the criminal activity would constitute an offence in Jamaica, if committed here and would be punishable by imprisonment for a maximum term in excess of twelve (12) months then the defence does not apply.

APPENDIX 1

SCHEDULE OF OFFENCES AND PENALTIES (POCA)[112]

The Proceeds of Crime Act, as well as the Schedule of Offences and Penalties can be accessed from the Ministry of Justice's website as outlined below:

The Proceeds of Crime Act
https://laws.moj.gov.jm/library/statute/the-proceeds-of-crime-act

The Proceeds of Crime (Amendment to the Second Schedule) Order, 2019
https://laws.moj.gov.jm/library/gazette/l-n-114g-2019

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/CPF legislation by adopting control procedures such as those outlined in the Guidelines. In determining whether a person has complied with the provisions of the AML legislation, (Regulations 3(3) and (4) of POC-MLPR, 2007) or theTPA legislation, (Regulation 3(1) and 3(2) of TP-RER, 2010), the court is required to take account of relevant Guidelines and consider whether the casino 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 businesses in the regulated sector to consult with the Competent Authority for the purpose of carrying out their obligations under Section 18, (Regulatory Controls by Certain Entities) of the TPA and POC-MLPR respectively.

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/TF/PF activities, costs to defend prosecutions, and costs to and costs to repair the institution's public image.

Loss of Reputation

Institutions that, even inadvertently, become involved in ML/TF/PF activities risk loss of their good name in the market. This may occur because of media coverage of the circumstances.

[112]Licensees are advised to review and keep advised of the Schedule of Offences in the POCA, as that legislation may be amended from time to time. Reliance on this Appendix is neither a defence to criminal prosecution arising from failure to comply with the POCA nor a mitigating factor in determining any penalty under the POCA.

APPENDIX 2

Additional roles of the Nominated Officer

Additional roles of the Nominated Officer include:

- preparing and updating policies and procedures and disseminating information to relevant persons;
- assisting in implementing compliance programmes;
- ensuring that risk assessments are kept up to date and relevant, and are carried out by the operator;
- ensuring that the operator's compliance programme complies with applicable laws, guidance from the CGC and the AML/CFT policies of the operator;
- ensuring that a risk profile (i.e. formal assessment of level of risk of money laundering) is established for customers, business relationships and one-off transactions and a determination made of which are high risk;
- implementing the relevant measures and mechanisms commensurate with the risks assessed;
- ensuring risk assessments;
- establishing procedures to assess the risk of money laundering arising from business/customer relationships, products/services and business practices (new or existing) and developing technologies and applied/used in respect of same;
- ensuring that special attention is paid to all business relationships and transactions with anyone resident domiciled in a territory specified in a list of applicable territories, published by notice in the *Gazette* by the Supervisory Authority (BOJ) and by virtue of the United Nations Security Council Resolutions Implementation Act;
- maintaining coordination between the Nominated Officers of each regulated entity within a group of companies/ related companies;
- Carrying out site visits to locations/branches/units to observe implementation of internal controls procedures;
- ensuring that the casino operator's enhanced due diligence procedures are appropriate;
- providing assistance to staff on AML/CFT issues that may arise in respect of new customers/patrons and business relationships;
- responding to internal and external enquiries in respect of the AML/CFT policies and procedures of the firm;
- ensuring implementation and observation of the internal controls and procedures;
- co-ordinating an annual audit of the AML/CFT/CPF programme to ensure compliance with all AML/CFT/CPF laws and requirement;
- ensuring that recommendations from any examination by the Competent Authority and internal/external auditors are promptly reported to the relevant internal body for review and are approved and implemented;
- co-ordinating with relevant persons e.g. on AML matters and investigations;
- acting as a liaison between the casino operator, the Competent Authority, and law enforcement agencies, with respect to compliance matters and investigations;
- evaluating new products and services (gaming devices, gaming services) to determine the risk exposure of the casino operator.

APPENDIX 3

Additional roles of the Nominated Officer

Possible methods of Money Laundering using Casino operations:[113]

- Use of casino value instruments such as chips, tokens, credits, casino cheques, etc.
- Structuring, rearranging or smurfing of transactions
- Refining of currency notes
- Use of individual customer accounts and safe deposit boxes
- Use of false or forged documents and means of payments
- Collusion in fixed games
- Other methods

1. Use of casino value instruments such as chips, tokens or cheques to launder money

Purchasing of casino chips or gaming credits with the intention of subsequent redemption of value of the instrument by way of payment documents such as cash, casino cheques or transferring back to bank or individual accounts.

- Money launderers, who, in ord to be customers of casinos will purchase casino chips with cash or bank transfers.
- Then they will make repayment requests in the form of cash, to a given bank account or by a casino cheque.

2. Money launderers who p tend as customers may purchase of chips or winnings from clean/genuine players at an attractive higher price:
    - Money launderers may purchase chips or winnings from customers with clean backgrounds who use the casino for gaming.
    - They will make very attractive proposals to purchase at a higher price than the face value of the chip.
    - This will make the arrangement favourable for both the seller and the buyer.
3. Casino chips are used as currency in illegal transactions:
    - Criminals may use casino chips, gift certificates and casino reward cards as currency to pay for illegal transactions such as purchasing of drugs, arms or payment for human trafficking.
    - The party who received the casino value instruments as the payment for such transactions can exchange them later at the casino businesses with least gaming or sometimes without gambling.

Structuring, rearranging or smurfing of transactions to launder money

1. Purchasing of casino chips regularly using cash:
    - Money launderers make regular cash payments with value below the threshold CDD limit which is UD$3,000 or equivalent in any other currency.
    - This is mainly to avoid the monitoring procedures of any financial transaction which is above the threshold CDD limit.
2. Money launderers may use third parties to undertake transactions:
    - Money launderers are sometimes organized groups.
    - They use one customer's account to transfer money to the casino in purchasing of chips.
    - Also, they make these payments which are just below the amount of CDD threshold reporting to avoid monitoring and possible questioning by the casino businesses.
3. Money launderers may be on alert of casino staff's work schedules to launder money without making any suspicion.
    - Money launderers may utilize staff movements and their work shift changes to conduct transactions.
    - They may trace the work schedules of casino staff, especially at cash desks and conduct transactions little below the customer identification threshold to avoid any monitoring or questioning.
    - Ex. Money launderers pretend as customers of casinos and will conduct transactions at the beginning of one work shift and at the end of another work shift of the cash desk employees.
4. Money launderers will regularly change the place of gaming to avoid possible suspicion on their behaviour:
    - Money launderers may attempt to regularly switch or exchange among gaming tables, gaming machines or gaming rooms when their wagering amounts closely approach the customer identification threshold.
5. Customers with the purpose of laundering money may request division of casino winnings:
    - Money launderers may prefer the amount of casino winnings, which exceeds the identification threshold, to be divided into cash or cheques below the threshold limit.
    - This is mainly to avoid the requirement of customer due diligence of cashouts which exceed the customer identification threshold.

[113]For the avoidance of doubt, the methods described in this Appendix are illustrative only, and are not exhaustive.

APPENDIX 3, *contd.*

Refining of currency notes

1. Exchanging currency notes at the cash desks/cashiers:
    - Members of the money laundering groups may individually approach the cash desk of the casino, and introduce themselves as customers for gaming.
    - They may ask to exchange low-denomination bills for higher-denomination ones.
    - In illegal businesses such as drug dealing, people get low-denomination currency notes.
    - It is hard to handle a large number of low-denomination currency notes.
    - Therefore, people involved in such illegal activities may use businesses like casinos to exchange their sale proceeds to high-value currency notes by pretending they are regular customers of the casino.
2. Money launderers can use gaming machines or currency note acceptors to refine currency:
    - Modern casinos have advanced gaming machines which consist of note acceptors.
    - These machines provide facilities to customers to add credits to their individual casino accounts/ to the casino's bank account.
    - These technologies could be used by money launderers to feed low-denomination currencynotes into the machine.
    - This will provide an accumulation of credit to the customer's individual account or to the casino's bank account.
    - Then, money launderers will redeem these accumulated credits with little or no gaming for high denomination banknotes.

Use of wire transfers and safe deposit boxes

1. Money launders may deposit cash into casino accounts by making wire transfers:
    - Funds are deposited into the customer's individual account/ casino account by a wire transfer from a local or foreign financial institution.
    - This enables the customer to freely make use of those funds, for gaming activities or any other service provided at the casino.
    - Money launderers may use such wire transfers to deposit money and with minimal or no gambling activity, request cash out from such balances of the casino account.
2. Money launderers may use foreign individual holding accounts to launder money in another jurisdiction:
    - There are casinos which have their chain of casino operations in other jurisdictions.
    - Those chains of casinos offer customers to hold individual accounts in one (1) country, for example, jurisdiction "A", but the funds can be used to purchase casino value instruments, as well as to be cashed out in jurisdiction "B" at a casino within the same chain.
    - In this case the money held in jurisdiction A's account does not leave the country physically or through electronic wire transfer.
    - This prevents the transaction from being monitored under the requirements of cash or wire transfer reporting requirements.
    - Also, if transactions are a little below the CDD threshold limit, then the identification threshold can also be avoided.
3. Potentials of money laundering using safety deposit boxes:
    - Casinos offer special services such as safety deposit boxes to their VIP or high-stakes players.
    - This service presents a money laundering risk due to a lack of transparency with the use of such boxes.
    - Also, there is possibility of providing access of these safety deposit boxes to third parties via a password or key.

Use of false/forged documents and means of payments

1. Potential of money laundering using false identification data:
    - Customer identification and verification of information is a legal requirement under the casino operations.
    - Money launderers may present false identification documents and made up personal data (e.g. address, phone number, occupation etc.) to conceal their real identity from these procedures.
    - Providing forged identities to customers may help money launderers misuse casino value instruments to launder money without any suspicion.
2. Use of forged means of payment:
    - Counterfeit currency notes or cheques can be used to purchase casino value instruments.

APPENDIX 3, *contd.*

- Also, non-cash means of payment such as forged credit cards or gift cards by means of identity theft e.g. bank account details, and passwords can be used to purchase casino value instruments with the intention of later converting them to cashouts with minimal gaming.

Collusion in fixed games

1. Making bets on fixed games with another customer:
    - There are well-organized money laundering groups who get involved in relatively low odds, low-risk games such as roulette, and blackjack.
        - This would involve two (2) or more pairs of players placing opposite equivalent bets on even money wagers in the same game.
        - • E.g., person "A" bets Rs. 100,000 on black, while person "B" bets Rs. 100,000 on red in a game of roulette.
        - Every loss for person "A" is a win for person "B", and vice versa.
        - This gaming method is also called the "intentional losses" method, when the loss of a player is factually reimbursed by the win of the associate player.
2. Making bets on fixed games with a casino employee:
    - Money launderers may collude with casino staffs to enable laundering of criminal proceeds without being detected.
    - Money launderers are willing to get the support of the casino staff in such activities (sometimes on a paid basis) as they would support them by avoiding filing reports over the threshold or reporting suspicious transactions.
    - Also, they would support by destroying documents related to customer due diligence or records on conducted transactions, falsifying gambling records on such customers, and arranging the game in a manner favourable for such customers.
    - Further, they will support such customers in fixed games with other players.

Indicators of money laundering in casino operations Red Flags/indicators of money laundering suspicions:

- Use of casino value instruments such as chips, tokens, credits, casino cheques, etc.
- Structuring, rearranging or smurfing of transactions
- Refining of currency notes
- Use of individual customer accounts and safe deposit boxes
- Use of false or forged documents and means of payments
- Collusion in fixed games
- Other methods

Indicators of money laundering suspicions related to the use of casino value instruments such as chips, tokens, gaming credits, casino cheques, etc.

- Customers who purchase casino value instruments and cash outs using them with little or no gaming activities.
- Customer exchanges cash for chips and vice versa multiple times during the same day.
- Customer purchases and cashouts chips similar or equal amount.
- Customer purchases chips and leaves the casino shortly after.
- Customers purchase chips through third parties.
- Detection of chips brought by customers into the casino from outside.
- Customer requests to add cash to casino winnings, and then exchanges the combined amount for a single cheque or bank draft.
- Customer purchases chips by depositing multiple cheques or bank drafts into individual accounts, or requests the winnings to be paid out in the form of multiple cheques or bank drafts.
- Customer inserts funds into gaming machines and claims those funds as credits on individual account/ cash with little or no gaming activity.
- Customer claims gaming machine credit payouts with no jackpot.
- Customer frequently inserts substantial amounts of cash in gaming machines that have high payout percentages and does not play "max bet" to limit chances of significant losses or wins, thereby accumulating gaming credits with minimal play.
- Customer requests transfer of credits to individual account with another casino.
- Abrupt changes in wagering or betting patterns.
- Customer's intention to win is absent or secondary.

APPENDIX 3, *contd.*

Indicators of Money Laundering suspicions related to the structuring, rearranging or smurfing of transactions

- Customers regular purchases of casino value instruments and frequent wagers in cash just below the identification threshold.
- A third party is present for all transactions of the customer.
- Customer allows third parties to use his/her individual account.
- Cash received from third party for purchasing chips.
- Cash handed to third party after exchanging chips.
- Transfer of funds from one individual account to multiple individual accounts.

Indicators of Money Laundering suspicions related to the refining of currency notes

- Customer in possession of large amounts of currency.
- Customers attempt to exchange low-denomination notes for high-denomination ones for various reasons.
- Customers insert low-denomination currency notes into note acceptors or gaming machines with little or no gaming activity before redeeming the credits for high denomination currency notes.
- Customers frequently deposit amounts in low-denomination currency notes on individual account with little or no play before-redeeming the balance of the account for high-denomination currency notes.

Indicators of Money Laundering Suspicions related to the use of individual accounts and safe deposit boxes

- Customer's cash deposits, cheques, and wire transfers into individual account/casino account inconsistent with customer profile.
- Customer withdraws funds from casino account shortly after being deposited (may request to transfer back to a given account number or to the same account number).
- Customers with significant movement of funds through the casino account with little or no gambling activity.
- Customer credits funds into a casino account from banks or other individual accounts in high-risk countries or from unknown sources.
- Customer may use intermediaries (authorized representatives) to undertake transactions.
- Funds are transferred to casino account/s from a corporate account/s.
- Customer regularly allows third parties to use the customer's safe deposit box.

Indicators of Money Laundering suspicions related to the use of false/forged documents and means of payment

- Customers introducing themselves under a fictitious name or different names.
- Customer may use identification documents with altered or missing entries.
- Inconsistent and contradictory identity information presented,
- Customer may refuse to present any identification document or personal data.
- Customers may use counterfeit currency notes or cheques for purchasing value instruments or replenishing individual accounts.
- Customer may use forged non-cash means of payment (e.g. debit, credit or gift cards) for purchasing value instruments.

Indicators of Money Laundering suspicions related to collusion in fixed games

- Even-money wagering when conducted by a pair of betters covering both sides of an even bet (e.g., in roulette, baccarat/mini-baccarat).
- Two or more pairs of customers frequently playing at the same table.
- Two or more pairs of players frequently wagering against one another (the win of one player is "accompanied" by the loss of the other).
- Customer attempting to befriend casino employees/staff.
- Customer prefers to play at the table serviced by a certain dealer/s.
- Contacts or connections between customers and casino employees/staff outside of the casino.

Other Indicators of Money Laundering in Casino Operations other Red Flags/Indicators of Money Laundering Suspicions:

- Transaction inconsistency with customer profile.
- High volume of transactions within a short period.
- Sudden increase in the volume of transactions.
- Customers pertaining to high-risk groups such as drug dealing, and contacts with PEPs.

APPENDIX 3, *contd.*

- Negative information on customers (Ex. Criminal Records).

Dated this 14th day of June, 2024.

CLOVIS METCALFE
Chairman
Casino Gaming Commission.

Approved:

HORACE CHANG
Minister of National Security.

PRINTED BY JAMAICA PRINTING SERVICES (1992) LTD., (GOVERNMENT PRINTERS), DUKE STREET, KINGSTON, JAMAICA