Table of Contents

THE

JAMAICA GAZETTE

EXTRAORDINARY

1429

Vol. CXXXVIII FRIDAY, JUNE 26, 2015 No. 32

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

DIONNE TRACEY DANIEL, (MRS.)
Governor-General's Secretary.

GOVERNMENT NOTICE

MISCELLANEOUS

No. 117

THE PROCEEDS OF CRIME ACT

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM GUIDELINES FOR CASINOS

In exercise of the powers conferred on the Honourable Minister of National Security, under section 94(7) of the Proceeds of Crime, Act 2007, has approved the following Guidance Notes for the Casino Gaming Industry:

1 INTRODUCTION AND LEGAL FRAMEWORK

1.1 INTRODUCTION

1.1.1 The Proceeds of Crime Act and the Proceeds of Crime (Money Laundering Prevention) Regulations, as amended in 2014 (Act 26 of 2013), imposes duties and responsibilities on businesses in the regulated sector to prevent and detect money laundering. By the Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013 with effect from 1st June, 2014 casino operators will be DNFI's and 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.

1.2 WHAT IS MONEY LAUNDERING

1.2.1 Money laundering generally refers to the methods and processes used by criminals to conceal the origin and ownership of the proceeds of their criminal activities. The purpose of money laundering is to allow criminals to maintain control over the proceeds of their crime and to ultimately give the appearance that these proceeds came from a legitimate source and from legal activities. There are three acknowledged stages to money laundering, that is 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 organisation as well as the available mechanisms for facilitating money laundering will determine the use of these three basic stages.

1.2.1.1 *Placement*

This is the stage 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.

1.2.1.2 *Layering*

This is the stage where the source of the criminal proceeds is obscured by creating layers of transactions designed to disguise the audit trail. 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.

1.2.1.3 *Integration*

This is the stage 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.

1.3 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, fund 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 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 relied efforts abroad, but, all the funds are actually transferred to a terrorist group. Funds may come, as well as from criminal sources, such as the drug trade, the smuggling of weapons and other goods, fraud, kidnapping and extortion. 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 establishes a number of terrorism offences including engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes.

1.4 INTERNATIONAL STANDARDS TO PREVENT MONEY LAUNDERING

1.4.1 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 created to tackle money laundering and terrorist financing. 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.

1.4.2 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[1]. 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]See FATF's website: http://www.fatf-gafi.org

1.4.3 The Caribbean Financial Action Task Force is an organisation 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 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), endorsed and agreed to implement the FATF Recommendations and to fulfil the obligations expressed in the Kingston Declaration On Money Laundering issued in November 1992 and agreed 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.

1.4.4 Recommendation 22 of the FATF Recommendations requires countries to regulate certain designated non-financial businesses and professions as part of its AML/CFT measures. Among the DNFBs to be regulated, FATF Recommendation 22(a) has identified casinos when customers engage in financial transactions equal to or above the applicable designated threshold.

1.5 IMPLEMENTATION OF THE UNITED NATIONS SECURITY COUNCIL RESOLUTIONS

1.5.1 Section 5 of The United Nations Security Council Resolutions Implementation Act requires DNFIs to ascertain whether they are in possession or control of assets owned or controlled by a proscribed individual or entity and to make reports to the Designated Authority at least once every four calendar months and/or in response to a request from the Designated Authority. At the date of this Guidance the form for the making of such report has not been prescribed.

1.5.2 The United Nations Security Council Resolutions Implementation (North Korea) Regulations also proscribed certain individuals and entities, and DFNIs are therefore obligated to ascertain whether they are in possession or control of assets owned or controlled by or on behalf of the proscribed individuals or entities.

1.5 THE JAMAICAN LEGAL FRAMEWORK ON MONEY LAUNDERING

1.6.1 The Proceeds of Crime Act (POCA) establishes a number of money laundering offences including:

(a) principal money laundering offences[2];

(b) offences of failing to report suspected money laundering[3];

(c) offences of tipping off about a money laundering disclosure, tipping off about a money laundering investigation and prejudicing money laundering investigations[4].

1.6.2 The principal money laundering offences are applicable to all persons whether or not they are regulated under POCA, however, the offences of failing to report suspected money laundering under sections 94 and 95 apply only to persons in the regulated sector.

1.6.3 The Proceeds of Crime (Money Laundering Prevention) 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 POCA (MLP) Regulations also create offences for breaches of the obligations imposed by the Regulations.

1.7 WHO COMPRISES THE REGULATED SECTOR

1.7.1 Businesses in the regulated sector include 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, and a designated non-financial institution (DNFI)[5].

(a) A FI is a bank licensed under the Banking Act; a financial institution licensed under the Financial Institutions Act; a building society registered under the Building Societies Act; a society registered under the Co-operative Societies Act; 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); a person licensed under the Bank of Jamaica Act to operate an exchange bureau; a person licensed under the Securities Act as a dealer or investment adviser; approved money transfer and remittance agents and agencies; the National Export Import Bank of Jamaica; and 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.

[2] POCA sections 92 and 93
[3] POCA sections 94, 95 and 96
[4] POCA section 97
[5] See section 16 of POCA (Amendment) Act 2013, which amends paragraph 1(1)(a) of the Fourth Schedule of POCA

(b) 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.

(c) In order to implement FATF Recommendation 22, The Proceeds of Crime (Designated Non-Financial Institution) (Casino Operators) Order, 2013, has been promulgated pursuant to powers conferred on the Minister by paragraph 1(2) of the Fourth Schedule of the POCA. Casinos have therefore been designated as non-financial institutions or DNFIs.

1.8 WHY CASINOS SHOULD BE REGULATED

1.8.1 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 areas:

1.8.1.1 *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 comingling of the deposit may also include other unrelated funds being laundered.

1.8.1.2 *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 exchange 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 amount in further attempt to hide the nature of the transaction.

1.8.1.3 *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 employee 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.

1.9 THE ROLE OF THE CASINO GAMING COMMISSION

1.9.1 The Casino Gaming Commission (the Commission) was established by the Casino Gaming, Act, 2010[6], 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[7] 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;

(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; and

(iii) facilitate responsible casino gaming; and

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

(e) advise the Minister on matters of general policy relating to casino gaming in Jamaica; and

(f) carry out such other functions pertaining to casino gaming as may be assigned to it by or under this Act or any other enactment.

[6] Sections 5
[7] Sections 6

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

- regulating casino gambling in the public interest;
- regulating in a transparent, accountable, consistent and targeted manner;
- assessing risk led by the evidence, relevant information and best regulatory practice in the light of international experience;
- consulting widely and effective use of resources.

1.10 POWERS OF THE CASINO GAMING COMMISSION AS COMPETENT AUTHORITY

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

1.10.2 The Act provides the Commission with powers to investigate the suitability of applicants and to maintain a rigorous licensing application procedure.[8] In particular the Commission 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.[9] A specified offence is defined in the Act to include offences including money laundering.

1.10.3 Further, the Commission is authorized to review licences[10] 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.[11]

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

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

(a) issuing a letter of warning, admonishment, censure or reprimand;

(b) revocation or suspension of a casino gaming licence; or

(c) variation of the terms of a casino gaming licence[12]. 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.[13]

1.10.6 The Commission is also authorized to give to 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.[14] The direction may require the casino operator to adopt, vary, cease or refrain from any practice in respect of the conduct of casino operations.[15] Where a casino operator fails to comply with a direction given he shall be liable on summary conviction in a Resident Magistrates' Court.[16]

1.11 THE SUPERVISORY AUTHORITY

1.11.1 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 sections 94 or 95 of 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.

1.12 STATUS OF THIS GUIDANCE

1.12.1 This Guidance is issued by the Commission as the Competent Authority for the use and benefit of casino operators. This Guidance represent the Commission's view of the effective measures that casino operators should follow to prevent and detect money laundering. This Guidance has been approved by the Minister and published in the *Gazette*. In accordance with section 94(7) of 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 POCA.

---

[8] Section 14
[9] Section 15(1)(c)
[10] Section 20
[11] Third Schedule (c) and (e)
[12] Section 2
[13] Section 27(1(b)(ii)
[14] Section 38(1)
[15] Section 38(3)
[16] Section 38(5)

While care has been taken to ensure that this Guidance is accurate, up to date and useful, the Commission will not accept any legal liability in relation to it. This Guidance does not relieve casino operators of the obligation to know and comply with AML/CFT Laws.

2 THE GUIDANCE

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 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 POCA and covers wide ranging circumstances involving any activity concerning the proceeds of any crime.

This includes:

- trying to turn money raised through criminal activity into 'clean' money (that is, classic money laundering);
- possessing or transferring the benefit of acquisitive crimes such as theft and fraud, and funds generated from crimes like tax evasion;
- possessing or transferring stolen goods;
- being directly involved with any criminal or terrorist property, or entering into arrangements to facilitate the laundering of criminal or terrorist property; and
- 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

2.2.1 **The POCA (MLP) Regulations[17] impose compulsory compliance requirements and a breach can constitute a criminal offence. However, within this legal framework of requirements, casinos have 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[18].**

2.2.2 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 and terrorist financing risks faced by the operator. These steps require the operator to:

- identify the money laundering and terrorist 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.

2.2.3 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 or terrorist financing. It focuses 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.

2.2.4 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 operator, along with robust mechanisms to ensure that they are carried out effectively, weaknesses are identified, and improvements are made wherever necessary.

Identifying and assessing the risks faced by the operator

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

- What risk is posed by the business profile and customers using the casino?

[17] POCA (MLP) Regulation 6
[18] POCA (MLP) Regulation 6(1)

- Is the business high volume consisting of many low spending customers?
- Is the business low volume with high spending customers, perhaps who use and operate within their cheque cashing facilities?
- 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?
- Are procedures in place to monitor customer transactions and mitigate any money laundering potential?
- Is the business local with regular and generally well known customers?
- Is there a large proportion of overseas customers using foreign currency or overseas based bank cheques or debit cards?
- Are customers likely to be individuals who hold public positions in other countries, that is, Politically Exposed Persons (PEPs)?
- Are customers likely to be engaged in a business which involves significant amounts of cash?
- Are there likely to be situations where the source of funds cannot be easily established or explained by the customer?
- Are there likely to be situations where the customer's purchase or exchange of chips is irrational or not linked with gaming?
- Is the majority of business conducted in the context of business relationships?

2.2.6 Deciding that a customer is presenting a higher risk of money laundering or terrorist financing does not automatically mean that he is a money launderer or a financier of terrorism. 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 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 to those whose income originates from their partner's employment or income).

2.2.8 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 materialise. Such additional information may include an understanding of where the customer's funds and wealth have come from.

2.2.9 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.

2.2.10 In order to be able to detect customer activity that may be suspicious, it is necessary to monitor transactions or activity[19]. 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.

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 money laundering and terrorist financing risks are kept under regular review.

2.3 SENIOR MANAGEMENT RESPONSIBILITY

Introduction

2.3.1 Senior management must be fully engaged in the processes around an operator's assessment of risks for money laundering and terrorist 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. Disregard for the legal requirements, for example, turning a blind eye to customers spending criminal proceeds, may result in criminal or regulatory action.

2.3.2 It is considered best practice, and is explicit in parts of the Regulations, that a risk-based approach should be taken to tackling money laundering and terrorist financing.

2.3.3 Operators, using a risk-based approach, should start from the premise that most customers are not money launderers or terrorist financiers. However, operators should have policies and procedures in place to highlight those customers who, according to criteria established by the operator, may present a higher risk. The policies and procedures should be proportionate to the risks involved.

[19] POCA (MLP) Regulation 7A

Obligations on all Operators

2.3.4 An officer of a licensed 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.

2.3.5 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.

Policies and procedures

2.3.6 Operators must establish and maintain appropriate written risk-based policies and procedures relating to:

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

2.3.7 The operator's policies and procedures should cover:

- the arrangements for nominated officer reports 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 both 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 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.

Training

2.3.8 The Regulations require that all relevant employees of casinos must be trained on the prescribed AML and CFT topics. 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.

2.3.9 One of the most important controls over the prevention and detection of money laundering 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.

2.3.10 Operators should devise and implement a clear and well articulated policy and procedure for ensuring that relevant employees are aware of their legal obligations in respect of the prevention of money laundering and terrorist financing, and for providing them with regular training in the identification and reporting of anything that gives grounds for suspicion of money laundering or terrorist financing.

2.3.11 Under POCA and the Terrorism Act, individual employees face criminal penalties if they are involved in money laundering or terrorist financing. If they do not make an internal report to their nominated officer when necessary they may also face criminal sanctions. It is important, therefore, that employees are made aware of their legal obligations, and are given training in how to discharge them.

2.3.12 The Regulations require operators to take appropriate measures so that all relevant employees are:

- made aware of the law relating to money laundering and terrorist financing; and
- regularly given training in how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

2.3.13 'Relevant employees' includes persons employed in specified offices as defined in the Casino Gaming Act and who are the holders of personal licences issued by the Commission as well as employees responsible for completing CDD measures. It does not include any ancillary employees such as catering and bar staff.

2.3.14 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 Commission will expect such issues to be covered in each operator's policies and procedures. This should make provision for the attainment of an appropriate competence level by the relevant employees identified in paragraph 3.13, prior to them undertaking the duties for which they will be responsible. This may, for example, be achieved by the attainment of an appropriate pass rate in a competency test following training.

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

- their responsibilities under the operator's policies and procedures for the prevention of money laundering and terrorist financing;
- the money laundering and terrorist 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.

2.3.16 There is no single solution when determining how to deliver training and a mix of training methods may, therefore, be appropriate. On-line 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.

2.3.17 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.

2.3.18 Ongoing training should be given to all relevant employees at appropriate intervals. Records should be maintained to monitor who has been trained, when they received the training, the nature of the training and the effectiveness of the training.

2.3.19 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.

2.4 NOMINATED OFFICER

2.4.1 The role of the Nominated Officer

2.4.1.1 The role of the Nominated Officer involves the development and implementation of programmes, policies, procedures and controls including:

- preparing and updating policies and procedures and disseminating information to relevant persons;
- assisting in implementing compliance programmes;
- ensuring that the operator's compliance programme complies with applicable laws, regulations, guidance from the Commission 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;
- 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);
- 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 of an annual audit of the AML/CFT programme;
- ensuring that recommendations from any examination by the Commission 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 Commission, and law enforcement agencies, with respect to compliance matters and investigations.

2.4.1.2 The role also involves ensuring the training of employees including:

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

2.4.1.3 The Nominated Officer has reporting functions including:

- seeking the consent of the Designated Authority (FID) in respect of transactions in accordance with the requirements of POCA and the POCA (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 operator, on AML/CFT issues; and
- preparing and submitting, at least on an annual basis, a comprehensive report to the senior management or other relevant persons within the operator, in respect of the effectiveness of the AML/CFT framework of the operator.

2.4.1.4 As well as monitoring functions, including:

- ensuring that record retention requirements and due diligence requirements are in keeping with AML/CFT laws, regulations 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 operator regarding the termination of customer or other business relationships and for the refusal to undertake new business from customers or other persons;
- 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 operator; and
- ensuring that enhanced monitoring is undertaken as required by the law, regulations or regulatory guidance, including but not limited to enhanced monitoring for high risk, persons.

2.5 CUSTOMER DUE DILIGENCE

2.5.1 A key requirement in the Regulations is the requirement to make checks on customers, known as customer due diligence or CDD[20]. Casino operators may take one of two approaches; identifying and verifying the identity of all customers on entry to the casino's licensed premises or undertaking identification and verification when a customer approaches the threshold set out in the Regulations.

2.5.2 Aside from these checks being a statutory requirement in the Regulations, they also make sense in terms of helping operators avoid the commission of criminal offences under POCA and other relevant legislation.

[20] POCA (MLP) Regulation 7A

2.5.3 CDD records held by a casino operator will need to be available across the operator's different casino premises and the policies and procedures must include details of how the operator will manage this. Operators should note that CDD is ongoing and may need updating for changes in the customer's circumstances and personal details.

Threshold Approach

2.5.4 The Regulations set out thresholds which, if customer transactions approach this level, require the casino operator to verify the identity of the customer. These limits are:

- in casinos the 'threshold approach for chips' — identification and verification is required when a customer purchases from or exchanges with the casino chips with a total value of US$3,000 or more during any period of 24 hours;
- in casinos the 'threshold approach for gaming machines' — identification and verification is required when a customer pays US$3,000 or more into the gaming machines during any period of 24 hours. This threshold amount does not include any winnings.

2.5.5 By separating the purchase or exchange of chips from the payment to use gaming machines there is the potential for customers to spend up to US$3,000 in the machines in addition to the purchase or exchange of chips up to US$3,000. It should be noted that for the purpose of this guidance 'gaming machine' and 'stake' have the same meaning as that in the Act.

2.5.6 If casinos wish to adopt the threshold approach, the following two conditions must be satisfied:

- it must verify the identity of each customer before, or immediately after, the customer purchases, exchanges, pays or stakes US$3,000 or more; and
- the Commission must be satisfied that the casino operator has appropriate procedures in place to monitor and record the total value of chips purchased from or exchanged with the casino, the total money paid for the use of gaming machines, or the total money paid or staked in connection with facilities for remote gaming by each customer.

2.5.7 Casino operators will have to satisfy the Commission that they have the mechanisms in place that are appropriate for the spend profile in each premises. For example, a casino with a customer drop/win average considerably below the threshold will need mechanisms in place to monitor customer transactions to be sure that any customer reaching either of the threshold levels is picked up in good time to allow CDD to be completed. Where the operator has a number of premises, the Commission will consider the use of the threshold approaches for each casino premises rather than for an operator.

2.5.8 Casinos adopting the threshold approach should think carefully about whether they wish to defer both identification and verification until the threshold is reached, or whether identification will be conducted on entry but verification deferred until the threshold is reached. For example, a premises based casino may operate a membership scheme where customers are identified on admission but verification only occurs once the threshold is approached.

2.5.9 There may be significant advantages in asking customers for their identification on entry, even if verification of this information is deferred until the threshold is reached, for example, identifying customers on entry means it will not be necessary to interrupt the customer's gambling once the threshold is reached, and verification becomes necessary.

2.5.10 Casinos have to monitor both purchase and exchange of chips. If either hits the threshold CDD will be necessary.

2.5.11 A key challenge for casinos wishing to adopt the threshold approach is keeping track of the level of all an individual customer's purchases and exchanges of chips, and spends on the gaming machines. However, it is appropriate to do so in light of the known spend patterns in each premises.

2.5.12 Should casino operators choose to adopt the threshold approach, they must satisfy the Commission, on a premises-by-premises basis, that they have the appropriate procedures in place to manage the threshold in light of the assessed money laundering risk and spending profile at each premises.

2.5.13 Casinos using the 'threshold approach' must be sure that they are able to end transactions with a customer who reaches the threshold if they are unable to comply with the CDD requirements.

2.5.14 The Commission has not determined the start of a 24 hour period for the purposes of the Regulations. Casino operators are free to choose the start time of their 24 hour period (previously referred to as the 'business day') to meet the demands of their business.

Identification and verification on entry

2.5.15 The 'on entry' approach requires casinos to identify and verify the identity of the customer before entry to any premises where gaming facilities are provided. Once the customer's identity is verified he may commence gaming.

2.5.16 If a casino using the 'on entry' approach to CDD is unable to complete the appropriate CDD they must not allow the customer access to the premises.

Identification and verification

2.5.17 Applying CDD measures involves several steps. The operator is required to identify customers and then verify their identities, either upon entry or when reaching the threshold. Identification of a customer is being told or coming to know of the customer's identifying details, such as their name and address. Verification is obtaining some evidence which supports this claim of identity. The operator identifies the customer by obtaining a range of information about him. The verification of the identity consists of the operator verifying some of this information against documents, data or information obtained from a reliable and independent source.

2.5.18 Identification of customers consists of a number of aspects, including the customer's name, current and past addresses, date of birth, place of birth, physical appearance, employment and financial history, and family circumstances.

2.5.19 Casino operators may identify their customers simply by asking them for personal information, including name, home address and date of birth. Other sources of identity can include:

- identity documents such as passports and photocard driving licences presented by customers;
- other forms of confirmation, including assurances from persons within the regulated sector (for example, banks) or employees within the same casino or casino group who have dealt with the customer for some time.

Some or all of this information will need to be verified. It may also be helpful to obtain information on customers' source of funds and level of legitimate income, for example occupation. This information may assist casinos with their assessments about whether a customer's level of gambling is in profile for their approximate income, or whether it is suspicious.

2.5.20 Information about customer identity must then be verified through documents, data and information which come from a reliable and independent source. There are a number of ways that a person's identity can be verified, including:

- obtaining or viewing original documents;
- conducting electronic verification;
- obtaining information from another person in the regulated sector (for example, banks).

No method of verification, either documentary or electronic, can conclusively prove that the customer definitely is who they claim to be. However, the Commission expects casinos to be reasonably satisfied following appropriate inquiry that customers are who they claim to be.

2.5.21 It is generally considered good practice to require either:

- one government document which verifies either name and address, or name and date of birth;
- a government document which verifies the customer's full name and another supporting document which verifies their name and either their address or date of birth.

Electronic verification

2.5.22 Increasingly casinos use reliable electronic systems to help with verification. Some of these systems also have the advantage of assisting in the identification of PEPs. The amount of electronic information available about individuals will vary, depending on the extent of their electronic 'footprint'.

2.5.23 Electronic data sources can provide a wide range of confirmatory material without necessarily requiring the customer to produce documents. Electronic sources can be a convenient method of verification. They can be used either as the sole method of verification, or in combination with traditional document checks, on a risk basis. For an electronic check to provide satisfactory evidence of identity on its own it must use data from multiple sources, and across time, or incorporate qualitative checks that assess the strength of the information supplied. An electronic check that accesses data from a single source (for example, a single check against the electoral roll) is not enough on its own to verify identity.

2.5.24 Some external electronic databases are accessible directly by casinos but it is more likely they will be purchased from an independent third party organisation. The size of the electronic'footprint' in relation to the depth, breadth and quality of data, and the degree of corroboration of the data supplied by the customer may provide a useful basis for an assessment of the degree of confidence in the product.

2.5.25 A number of commercial agencies which access many data sources are accessible online by operators, and may provide operators with a composite and comprehensive level of electronic verification through a single interface. Such agencies use databases of both positive and negative information, and many also access high-risk alerts that utilise specific data sources to identify high-risk conditions, for example, known identity frauds or inclusion on a sanctions list.

2.5.26 Positive information (relating to full name, current address, date of birth) can prove that an individual exists, but some can offer a higher degree of confidence than others. Such information should include data from more robust sources — where an individual has to prove their identity, or address, in some way in order to be included, as opposed to others, where no such proof is required.

2.5.27 Negative information includes consideration of lists of individuals known to have committed fraud, including identity fraud, and registers of deceased persons. Checking against such information maybe appropriate where other factors suggest an increased risk of impersonation fraud.

Criteria for use of electronic data provider

2.5.28 Before using a commercial agency for electronic verification, operators should be satisfied that information supplied by the data provider is considered to be sufficiently extensive, reliable and accurate. This judgement may be assisted by considering whether the provider meets all the following criteria:

- it is internationally recognised, and registered [with the appropriate body];
- it uses a range of positive information sources that can be called upon to link an applicant to both current and previous circumstances;
- it accesses negative information sources, such as databases relating to identity fraud and deceased persons;
- it accesses a wide range of alert data sources; and
- it has transparent processes that enable the operator to know what checks were carried out, what the results of these checks were, and what they mean in terms of how much certainty they give as to the identity of the subject.

2.5.29 In addition, a commercial agency should have processes that allow the enquirer to capture and store the information they used to verify identity.

2.5.30 It is important that the process of electronic verification meets a standard level of confirmation before it can be relied on. The standard level of confirmation, in circumstances that do not give rise to concern or uncertainty, is:

- one match on an individual's full name and current address; and
- a second match on an individual's full name and either his current address or his date of birth.

2.5.31 Commercial agencies that provide electronic verification use various methods of displaying results — for example, by the number of documents checked, or through scoring mechanisms. Operators should ensure that they understand the basis of the system they use, in order to be satisfied that the sources of the underlying data meet the required standard.

Documentary evidence

2.5.32 If verification is undertaken using documents, casino operators should usually rely upon documents issued by government departments.

2.5.33 Original documents should be examined so that, as far as reasonably practicable, forgeries are not accepted. Casino operators should recognise that some documents are more easily forged than others. If suspicions are raised in relation to any document offered, operators should take whatever practical and proportionate steps are available to establish whether the document offered is a forgery or has been reported as lost or stolen. While the presentation of false documents does not, in itself, amount to money laundering, it may constitute an offence under the Forgery Act and should, in appropriate circumstances, be reported to the police or FID. Casino operators should also be aware that even if documents appear to be legitimate and issued by a government department they may be false. Commercial software is available that checks the algorithms used to generate passport numbers. This can be used to check the validity of passports of any country that issues machine-readable passports.

2.5.34 If documents are in a foreign language appropriate steps should be taken to be reasonably satisfied that the documents in fact provide evidence of the customer's identity, for example, a translation of the relevant sections.

2.5.35 Documentation purporting to offer evidence of identity may emanate from a number of sources. These documents differ in their integrity, reliability and independence. Some are issued after CDD on the holder of the document is carried out by the issuing authority. There is a broad hierarchy of documents.

2.5.36 Documents issued by government departments and agencies that contain a photograph may be considered reliable. In practical terms, for face-to-face verification conducted by casinos, production of a valid passport or photocard driving licence should enable most individuals to meet the identification requirement for AML/CFT purposes. These documents will also confirm either residential address or date of birth.

2.5.37 Alternatively government issued documents without a photograph may be used which incorporates the customer's full name, supported by a second document, which is ideally also government issued, or issued by a public sector body or authority. This second document must also include the customer's full name and either his residential address or his date of birth.

2.5.38 The following sources may, therefore, be useful for verification of Jamaican-based customers:

- current signed passport;
- birth certificate;
- current drivers' licence;

- voters' ID card;
- utility bill or statement.

2.5.39 Customers who are not resident in Jamaica should be asked to produce their passport, national identity card or photocard driving licence. If the operator has concerns that the identity document or photo driving document presented by a customer is not genuine, they should contact the relevant embassy or consulate. Confirmation of the customer's address can be obtained from:

- an official overseas government source;
- a reputable directory of addresses;
- a person regulated for money laundering purposes in the country where the customer is resident (for example, a casino or bank) who confirms that the customer is known to them and lives or works at the overseas address supplied.

Politically Exposed Persons

2.5.40 A Politically Exposed Person (PEP) is a person who is or has, at any time in the preceding year, been entrusted with prominent public functions domestically or by a state outside Jamaica, a Community institution (for example, CARICOM) or an international body (for example, the United Nations), including the following persons:

- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliament;
- members of supreme courts, constitutional courts or other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exception circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors, charge d'affairs and high ranking officers in armed forces;
- members of the administrative, management of supervisory bodies of state-owned enterprises.

The following persons are also regarded as PEPs by virtue of their relationship or association with the persons listed above:

- family members of the persons listed above, including spouse, partner, children and their spouses or partners, and parents;
- known close associates of the persons listed above, including persons with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relationships, or who is a sole beneficial owner of a legal entity or arrangement set up by the PEP with whom they are associated.

PEP status itself does not incriminate individuals or entities. It does, however, put a customer into a higher risk category.

Risk-based approach to PEPs

2.5.41 The nature and scope of a particular casino's business will help to determine the likelihood of PEPs in their customer base, and whether the operator needs to consider screening all customers for this purpose.

2.5.42 Establishing whether individuals are PEPs is not always straightforward and can present difficulties. Where operators need to carry out specific checks, they may be able to rely on an internet search engine, or consult relevant reports and databases on corruption risk published by specialised national, international, non-governmental and commercial organisations. Resources such as the Transparency International Corruption Perceptions Index, which ranks approximately 150 countries according to their perceived level of corruption, may be helpful in assessing the risk.

This can be found at *www.transparency.org/policy research/surveys indices/cpi.*

If there is a need to conduct more thorough checks, or if there is a high likelihood of an operator having PEPs for customers, subscription to a specialist PEP database may be a valuable tool in assessing the risk.

2.5.43 New and existing customers may not initially meet the definition of a PEP, but that position may change over time. Equally, individuals who are initially identified as PEPs may cease to be PEPs, for example, a year after they change their job or retire. The operator should, as far as practicable, be alert to public information relating to possible changes in the status of its customers with regard to political exposure. Casino operators should be alert to situations which suggest that the customer is a PEP. These situations include:

- receiving funds from a government account;
- correspondence on an official letterhead from the customer or a related person;
- general conversation with the customer or related person linking the person to a PEP;
- news reports suggesting that your client is a PEP or is linked to one.

2.5.44 Although under the definition of a PEP an individual ceases to be so regarded after he has left office for one year, operators are encouraged to apply a risk-based approach in determining whether or when they should cease carrying out appropriately enhanced monitoring of transactions. In many cases, a longer period might be appropriate, in order to ensure that the higher risks associated with the individual's previous position have adequately abated.

2.5.45 Each operator's policies and procedures should cover when and how customers will be checked for PEP status.

PEPs requirements

2.5.46 An operator who proposes to allow a PEP to be a customer must:

- have approval from its senior management for establishing a business relationship with that person;
- take adequate measures to establish the source of wealth and source of funds which are involved in the proposed business relationship; and
- where a business relation is entered into, conduct enhanced ongoing monitoring of the relationship.

2.5.47 Each operator's policies and procedures should cover how and when senior management approval will be sought and provided, and deal with how the customer will be dealt with if there is any delay to approval being provided.

Failure to complete checks

2.5.48 Where a casino operator is unable to comply with the required CDD measures in relation to a customer, the operator:

- must not carry out a transaction with or for the customer through a bank account;
- must not establish a business relationship or carry out an occasional (one-off) transaction with the customer;
- must terminate any existing business relationship with the customer; and
- must consider making a report to FID.

2.5.49 Casinos must therefore have clear policies in place on how they will manage situations where they are unable to comply with the CDD measures.

2.6 RECORD KEEPING

General legal and Regulatory Requirements

2.6.1 This chapter provides guidance on appropriate record keeping procedures required by the Regulations. The purpose of the record keeping requirement is to ensure that there is an audit trail that could assist in any financial investigation by a law enforcement body.

2.6.2 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 why no further action was taken;
- 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.

2.6.3 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 is either:

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

Business relationships

2.6.4 Casino operators form business relationships with their customers if, at the point that contact is established, the casino expects their relationship to have an element of duration. Casino operators are encouraged to interpret this definition widely.

2.6.5 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.

2.6.6 '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[21].

2.6.7 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.

Occasional transaction/One-off Transactions

2.6.8 A casino may undertake an occasional transaction with a customer when there is no business relationship but the customer purchases or exchanges chips over US$3,000.00 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 US$3,000.00 limit constitutes an 'occasional 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 five years after the date of the visit.

Other Casino Customers

2.6.9 Some casino customers may not fall into the business relationship or occasional 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.

Customer information

2.6.10 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.

2.6.11 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.

2.6.12 There is a separate requirement in the Regulations to ensure that documents, data or information held by casinos are kept up to date[22]. 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 picked up. Keeping information up to date is also a requirement under 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.

Supporting records

2.6.13 The requirement to keep supporting records is linked to 'business relationships' and 'occasional transactions' which are defined in the Regulations[23] 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 occasional 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.

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

2.6.15 Any casino operator devising its record keeping policy and procedure should decide how its business fits within the definitions of 'business relationship' or 'occasional 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.

2.6.16 For the purposes of supporting records, the Commission takes the view that in most cases this will consist of records covering the drop/win figures, subject to paragraph 2.6.9, 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 Commission may require operators to maintain records for each table or game but not broken down by each customer's transactions.

Supporting records — gaming machines

2.6.17 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

[21] POCA (MLP) Regulation 7A
[22] POCA (MLP) Regulation 7A
[23] POCA (MLP) Regulation 7A

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.

2.6.18 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.

2.6.19 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.

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

2.6.20 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.

2.6.21 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.

Retention period

2.6.22 Records of identification and verification of customers must be kept for a period of at least seven years[24] after the relationship 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.

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

Form in which records have to be kept

2.6.24 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.

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

2.6.26 Where the record keeping obligations under the Regulations are not observed, an operator or person is open to prosecution and sanctions, including imprisonment and/or a fine, or regulatory censure.

2.7 SUSPICIOUS ACTIVITIES AND REPORTING

Introduction

2.7.1 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'.

2.7.2 In order to provide a framework within which suspicion reports 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;

[24] Prevention of Crime (Money Laundering Prevention) Regulation, 2007, Regulation 14(5)(a)

- 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.

2.7.3 If the nominated officer determines that a report does give rise to grounds for knowledge or suspicion, he must report the matter to FID. Under POCA, the nominated officer is required to make a report to FID as soon as is practicable if he has grounds for suspicion that another person, whether or not a customer, is engaged in money laundering. Under the Terrorism Act, similar conditions apply in relation to disclosure where there are grounds for suspicion of terrorist financing.

What is meant by knowledge and suspicion?

2.7.4 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 obligation to make a report. This does not preclude a report being made should employees choose to do so. Employees may also be obliged to make a report by other parts of the Act.

2.7.5 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.'*

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.

2.7.6 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.

2.7.7 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.

2.7.8 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.

What is meant by reasonable grounds to know or suspect?

2.7.9 In addition to establishing a criminal offence relating to when 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 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.

2.7.10 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.

Internal reporting

2.7.11 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 as soon as possible.

2.7.12 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.

2.7.13 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 obligations.

Evaluation and determination by the nominated officer

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

2.7.15 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 accidently.

External reporting

2.7.16 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.

2.7.17 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 days after the information or other matter came to the nominated officer.

Submission of suspicious activity reports

2.7.18 FID accepts the submission of STRs in two ways:

- 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 properly addressed. Failure to do so may result in unauthorized disclosures.
- Online Reporting POCA (MLP) Regulation 17 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.

2.7.19 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 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 number)
- Jamaican Dollar equivalent
- US Dollar Equivalent
- Reasons for suspicion (for STRs)

2.7.20 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.

Appropriate consent

2.7.21 If operators handle any proceeds of crime they may commit one of the principal money laundering offences in POCA or the Terrorism Prevention Act. 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'[25].

2.7.22 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 of 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.

[25] POCA section 99

2.7.23 Consent should be requested through the completion and submission of an authorized disclosure (Form 111), to the FID.

Proceeding with Transactions after Consent has been Requested

2.7.24 The Nominated Officer may give the appropriate consent to the doing of a prohibited act in instances where the 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.

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 faxed or 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.

Future Requests for Consent for the same Customer

2.7.25 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.

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.

Communicating with Customers during the Consent Period

2.7.26 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:

(a) During the notice period (seven working days), that the transaction is being delayed because it is awaiting consent from the designated authority;

(b) During the 10-day moratorium period, that consent was refused by the designated authority;

(c) At a later date, that the transaction was delayed because the consent of the designated authority was being sought; or

(d) That law enforcement is conducting an investigation.

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.

22.7.27 Reporting suspicious activity before or reporting after the event are not equal options which an operator can choose between. A report made after money laundering 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. Where a customer 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 working day notice period from the working day following the date of disclosure, unless FID gives consent.

2.7.28 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 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.

2.7.29 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 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.

2.7.30 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 POCA or the Terrorism Prevention Act, as well as potential damage to reputation and other commercial factors.

2.7.31 Operators should also note that in the Commission'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.

2.7.32 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 under the Regulations 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.

2.7.33 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.

Tipping off, or prejudicing an investigation

2.7.34 Under section 97 of POCA a person commits an offence if:

(a) the person knowing or having reasonable grounds to believe that a disclosure falling within section 100 has been made, he makes a disclosure which is likely to prejudice any investigation that might be conducted following the first mentioned disclosure; or

(b) the person knowing or having reasonable grounds to believe that the enforcing authority 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.

(c) the information on which the disclosure is based came to the person in the course of a business in the regulated sector.

A person also commits an offence under section 333A if:

(a) the person discloses that an investigation into allegations that an offence under Part 7 of POCA has been committed, is being contemplated or is being carried out;

(b) the disclosure is likely to prejudice the investigation; and

(c) the information on which the disclosure is based came to the person in the course of a business in the regulated sector.

2.7.35 Under section 104 of POCA a person in the regulated sector also commits an offence if he:

- knows or suspects that an appropriate officer is acting (or proposing to act) in connection with a confiscation investigation, a civil recovery investigation, a detained cash investigation or a money laundering investigation which is being or is about to be conducted; and
- 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.

2.7.36 Under POCA, a person does not falsify, conceal, destroy or otherwise dispose of, or cause or permit the falsification, concealment, destruction or disposal of, documents which are relevant to the investigation if he:

- does not know or suspect that the documents are relevant to the investigation;
- does not intend to conceal any facts disclosed by the documents from any appropriate officer carrying out the investigation.

2.7.37 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. There are a number of disclosures which are permitted and that do not give rise to these offences (permitted disclosures) — see POCA section 97 and 104(4)(3).

2.7.38 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. An offence is not committed if the person does not know or suspect that the disclosure is likely to prejudice an investigation, or if the disclosure is permitted under POCA or the Terrorism Prevention Act. 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.

2.7.39 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 POCA or the Terrorism Prevention Act.

2.7.40 An offence is not committed under POCA or the Terrorism Prevention Act if the disclosure is made to the relevant supervisory authority (the Commission) for the purpose of:

- the detection, investigation or prosecution of a criminal offence in Jamaica or elsewhere
- an investigation under POCA
- the enforcement of any order of a court under POCA.

2.7.41 An employee, officer or partner of a casino operator does not commit an offence under POCA or the Terrorism Prevention Act if the disclosure is to an employee, officer or partner of the casino operator.

2.7.42 A person does not commit an offence under POCA or the Terrorism Act if the person does not know or suspect that the disclosure is likely to prejudice:

- any investigation that might be conducted following a disclosure; or
- an investigation into allegations that an offence under Part V of POCA or Section 17 of the Terrorism Prevention Act has been committed, is being contemplated or is being carried out.

2.7.43 The fact that a transaction is notified to FID before the event, and FID does not refuse consent within seven 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.

2.7.44 This means that an operator:

- cannot, at the time, tell a customer that a transaction is being delayed because a report is awaiting consent from FID;
- 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
- cannot tell the customer that law enforcement is conducting an investigation.

2.7.45 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.' It was further observed that the 'truth is that Parliament has struck a precise and workable balance of conflicting interests in the 2002 Act'. The Court appears to have approved of the seven and 31 day scheme and said that in relation to the limited interference with private rights that this scheme entails 'many people would think that a reasonable balance has been struck'.

2.7.46 The existence of a STR cannot be revealed to any customer of the casino at anytime, 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.

2.1.47 The combined effect of these two offences is that one or other of them can be committed before or after a disclosure has been made.

2.7.48 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 months then the defence does not apply.

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.
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.
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 & Planning, 1 Shalimar Avenue, Kingston
DNFBP	Designated Non-Financial Businesses and Professions
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.
Operators	Firms holding an operator's licence issued by the Commission.
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.
STR	A Suspicious Transaction Report- the means by which suspicious activity relating to possible money laundering or the financing of terrorism is reported to FID under POCA or the TPA.
The Commission	The Casino Gaming Commission
The Regulations	The Proceeds of Crime (Money Laundering Prevention) Regulations Regulations made pursuant to the Casino Gaming Act, 2010
TPA	Terrorism Prevention Act

Dated this 26th day of June, 2015.

WALTER SCOTT, QC
Chairman
Casino Gaming Commission.

Approved:

PETER BUNTING
Minister of National Security.