BETTING, GAMING AND LOTTERIES COMMISSION

ANTI-MONEY LAUNDERING

GUIDANCE NOTES

FOR

GAMING LOUNGE OPERATORS

EXPLANATORY FOREWORD

All licensees of the Betting, Gaming and Lotteries Commission (Commission) have a responsibility to not allow their businesses to be used by criminal elements to launder the proceeds of crime. However, gaming lounge operators have additional and specific responsibilities under the Proceeds of Crime Act and the Proceeds of Crime (Money Laundering Prevention) Regulations.

The Commission has been designated the Competent Authority under POCA. As the competent authority, the Commission has a duty to supervise gaming lounge operators to ensure that adequate measures are in place to prevent the gaming lounges from being used for money laundering and terrorism financing and to aid them in detecting money laundering.

The Commission has powers to issue directives to gaming lounge operators and issues this guidance note in that light. The purpose of the guidance note is to provide detailed guidance on the requirements of POCA and practical guidance on how to implement such requirements into their daily operation.

The Commission uses a risk based approach to supervising gaming lounges; as such, it intends to issue periodic directions to licensees to supplement this guidance note as money laundering risks evolve. However, all guidance notes issued, must be read in conjunction with the relevant legislations.

GLOSSARY

"AML" means anti-money laundering

"CDD/KYC" means customer due diligence/ know your clients/customers

"CFATF" means the Caribbean Financial Action Task Force

"CFT" means combating of terrorism financing

"COMMISSION" means the Betting, Gaming and Lotteries Commission

"CRIMINAL CONDUCT"

This means conduct occurring on or after the 30th May, 2007, being conduct which –

(a) constitutes an offence in Jamaica;

(b) occurs outside of Jamaica and would constitute such an offence if the conduct occurred in Jamaica; [s. 2 POCA]

"CRIMINAL PROPERTY"

Property is criminal property if it constitutes a person's benefit from criminal conduct or represents such a benefit, in whole or in part and whether directly or indirectly (and it is immaterial who carried out or benefitted from the conduct).[s. 91 POCA]

"**DA**" means the Designated Authority who is the Chief Technical Director at the FID

"EDD" means enhanced due diligence

"FID" means the Financial Investigations Division

"FT" means terrorism financing

"ML" means money laundering

"MONEY LAUNDERING"

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.

Methods of laundering range from relatively simple transactions such as the purchase and resale of real property and luxury items to complex layers of transactions involving the establishment of different kinds of legal vehicles and cross border movement of funds through various accounts and business transactions. Despite the variety of methods that can be employed, the laundering process has three identifiable stages, that is, placement, layering and integration. These steps may occur as separate and distinct or may occur simultaneously. It is not uncommon for the steps to overlap, however the requirements of the criminal or the

criminal organisation as well as the available mechanisms for laundering will determine the use of these three basic stages.

"PEPs" means politically exposed persons

"POCA" means the Proceeds of Crime Act

"PROCEEDS OF CRIME"

Generally speaking, the term 'proceeds of crime' refers to the property obtained from a direct or indirect engagement in a criminal activity. For example, property obtained from a drug deal or a robbery.

"TERRORISM FINANCING"

Terrorism financing is the provision or collection of funds by a person, whether directly or indirectly, wilfully and without lawful justification or excuse, to be used in carrying out any terrorism activity.

Terrorism activity includes:

- causing death or serious bodily injury to a person;
- endangering a person's life, or the health and safety of the public;
- causing substantial property damage which results in death or serious bodily injury to a person, or endangers a person's life or the health or safety of the public.

The motive for the act must be political, religious or ideological.

Terrorism financing focuses on the destination of funds whereas money laundering focuses on the origin of funds.

"**TPA**" Terrorism Prevention Act

TABLE OF CONTENTS

PART ONE

BACKGROUND

The Proceeds of Crime Act, 2007 (POCA) and the Proceeds of Crimes (Money Laundering Prevention) Regulations 2007 ("the Regulations") impose duties and responsibilities on businesses in the regulated sector to prevent and detect money laundering.

Businesses in the regulated sector fall under two categories, viz., a financial institution (FI) and a designated non-financial institution (DNFI).

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 for the purposes of the Act.

On the 19th of November, 2013, the Minister of National Security, by Order, designated any person who operates twenty (20) or more gaming machines (gaming lounge) pursuant to a licence under the Betting, Gaming and Lotteries Act as a DNFI for the purposes of POCA and the Regulations. Therefore, all gaming lounge operators have a legal obligation to mitigate against ML/FT risks.

See Appendix1: The Proceeds of Crime (Designated Non-Financial Institution) (Gaming Machine Operators) Order, 2013.

The Minister of National Security also has the power under POCA to appoint, in writing, an authority to monitor compliance by a DNFI with the requirements of POCA and the Regulations as well as issue guidelines to a DNFI regarding effective measures to prevent money laundering. This authority is referred to as the **Competent Authority**.

On April 1, 2014, The Betting, Gaming and Lotteries Commission ("the Commission") has been designated the Competent Authority empowered to monitor the compliance of its gaming lounge operators with POCA and its regulations. **See Appendix 2: Letter dated February 5, 2014 from the Minister of National Security.**

<u>The purpose of the guidance note</u>

As a Competent Authority, the Commission is empowered to issue directions to DNFI's licensees for the purpose of securing compliance with the provisions of POCA and all regulations made under POCA. A failure to comply with any requirement or direction issued by the Commission will amount to an offence and liability for a fine.

Also, failure to comply with regulations under POCA and the TPA will constitute an offence and a court in determining whether a person has complied with any of the requirements of these regulations shall take into account any relevant guidance that was at the time concerned:

- issued by the Designated Authority or a body that regulates, or is a representative of, any trade, profession, business or employment concerned;
- approved by the minister; and

- published in the Gazette.

The directions contained in this guidance note, therefore apply to all persons who operate twenty or more gaming machines on any prescribed premises under a licence issued by the Commission pursuant to the Betting, Gaming and Lotteries Act ("BGLA"), (hereinafter "gaming machine operators"). This guidance note highlights the duties and obligations of licensees under POCA and its regulations, explains how such duties and obligations can be fulfilled, instructs licensees to devise their own policies and procedures to fulfil these obligations. Hence, outlined in this guidance note are requirements for record keeping, identification and verification of customers, monitoring of customers account and activity, nomination of a nominated officer, the report of all suspicious activities and significant transactions and cooperation with enforcement officers.

LEGAL FRAMEWORK

The Laws of Jamaica relating to ML and FT are contained in:

The Proceeds of Crime Act, 2007 and 2013 Amendments

The Proceeds of Crime (Money Laundering Prevention) Regulations 2007, and 2013 Amendments

The Terrorism Prevention Act, 2005 and 2011, 2012 and 2013 Amendments

Financial Investigations Division Act, 2010 and 2013 Amendments

Copies of the above and other laws can be found at www.moj.gov.jm and www.japarliament.gov.jm

The Proceeds of Crime Act, 2007 (POCA)

POCA establishes a number of money laundering offences including:

- principal money laundering offences of engaging in a transaction involving any asset or benefit derived from the commission of a crime;
- offences for failing to report suspected money laundering;
- offences of tipping off about a money laundering disclosure or investigation; or prejudicing a money laundering investigation.

POCA applies to all persons, however failure to report offences, tipping off offences, and the offence of failure to establish certain regulatory controls only apply to FIs and DNFIs.

The Proceeds of Crime (Money Laundering Prevention) Regulations, 2007

The Regulations set out requirements for FIs and DNFIs to:

- put in place procedures to verify the identity of customers on entering into a business relationship or transaction;

- verify the purpose and nature of transactions and carry out ongoing monitoring during the business relationship;
- keep records of identification and of the business relationship for seven years;
- appoint a nominated officer whose responsibilities include the reporting of suspicious activities to the Designated Authority (the Chief Technical Director of the Financial Investigations Division);
- put in place policies and procedures to prevent and detect money laundering and carry out independent audits from time to time to ensure compliance with all relevant anti-money laundering programmes, policies and procedures;
- carefully check the personal and financial history of employees;
- train employees in the relevant procedures and the law.

The Terrorism Prevention Act, 2005 (TPA)

TPA establishes a number of terrorism offences including: principal terrorism offences; offences of tipping off about a terrorism disclosure or investigation; and offences of prejudicing a terrorism investigation. The Act requires foreign companies carrying out banking, securities, investment advice or trusts, FIs, and any entity designated by the Minister of Foreign Affairs as an entity to which reporting requirements are mandated, to report on a continuing basis all information pertaining to listed entities as well as suspected terrorist activities. Entities must vet the personal and financial history of employees and put in place other regulatory controls to detect and prevent the financing of terrorism.

The Terrorism Prevention (Reporting Entities) Regulations, 2010

TPA (RE) Regulations set out requirements for the identification of customers; verification of the purpose and nature of transactions; and record keeping and reporting procedures.

Both POCA and TPA are part of a legislative regime designed to combat the laundering of the proceeds of crime, terrorism activities, and other serious crimes. Other legislation of relevance to anti-money laundering and combating the financing of terrorism include inter alia:

- The Dangerous Drugs Act, 1948
- The Extradition Act, 1991
- The Financial Investigations Division Act, 2010
- The Firearms Act, 1967
- The Mutual Assistance (Criminal Matters) Act, 1995

- The Sharing of Forfeited Property Act, 1999;

as well as other legislation relating to fraud, dishonesty, and corruption.

DESIGNATED AUTHORITY

The Chief Technical Director of the Financial Investigations Division (FID), Ministry of Finance and Planning was named the Designated Authority to receive reports as per sec 91(1) (h) of the Proceeds of Crime Act, Sec 15(1) of Terrorism Prevention Act and Sec 5(1) of the UN Act:

a) Suspicious Transaction Report (POCA Sec 94 & 95)

b) Threshold Transactions Report (POCA MLP Regulations section 3)

c) Authorized Disclosure (POCA Sec 100(4)

d) Report of International Transportation of Currency or Bearer Negotiable Instruments (POCA Section 101);

e) Suspicious Transaction Report (TPA Sec 16)

f) Listed Entity Report (TPA Sec (15)(3)

g) UN Security Council Proscribed Person or Entity Report (UN Act Sec 5(3)

COMPETENT AUTHORITY

The Role of the Commission

While suspicious transactions are to be reported to the DA and FID (and whoever else) have responsibility for investigating ML and FT breaches, the Commission, as the CA, has a duty to monitor the compliance of licensees with the requirements of Part V of POCA and regulations made thereunder and to issue guidelines regarding effective measures to prevent ML[1]. This guidance note is a tool in carrying out that duty.

Powers of the Competent Authority

The Competent Authority is empowered to:

- carry out inspections, whether on its own, or through a third party, of the business of a licensee;

[1] Section 91(1)(g)

- issue directions to a licensee including directions to take such measures as are necessary to prevent, detect, or reduce the risk of money laundering or terrorism financing;

- examine and take copies of information or documents in the possession or control of any licensee relating to the operations of that licensee;

- share any examination conducted by it with another competent authority, a Supervisory Authority or the Designated Authority, or an authority in another jurisdiction exercising functions similar to those of any of the aforementioned authorities –

    - but not information which is protected from disclosure under the Act or any other law: and

    - in order to prevent disclosure of the protected information or to prevent compromising or obstruction of any investigation in relation to an offence under the Act or any other law, make the sharing of information subject to any terms, conditions or undertakings which it thinks fit;

    - require by notice in writing, that a licensee registers with it any particulars that may be prescribed and/or make reports in respect of matters specified in the notice.

The power of the Competent Authority to examine and take copies of information in the possession or control of any licensee does not extend to information or advice that is subject to legal professional privilege. POCA explicitly provides that information or advice that is subject to legal professional privilege does not include information or any other matter that is communicated or given with the intention of furthering a criminal purpose.

Please note, that where a licensee is convicted of the offence of failing to comply with any requirements or directions issued by the Competent Authority, the conviction for the offence is deemed to be grounds for suspension or cancellation of its licence.

PART TWO

RISK-BASED APPROACH

Introduction

The FATF Recommendations support the adoption of a risk-based approach to combating ML and terrorism financing. By adopting a risk-based approach, competent authorities and regulated businesses have to develop capabilities to ensure that measures to prevent or mitigate ML and terrorism financing risks are commensurate to the risks identified. Therefore, higher risks would receive greater attention.

RISK-BASED APPROACH TO SERVICES AND BUSINESS PRACTICES (see amended Regulations 6 and 7of POCA (MLP) Regulations)

Regulated businesses are prohibited from forming business relationships or carrying out a one off transaction with or for another person unless the business maintain procedures to assess the risk of money laundering arising from its products/services and business practices (whether new or existing) and developing technologies applied or used in such products or practices.

A risk based approach to ML/FT involves implementing clearly defined and discrete policies and procedure for detecting, preventing and mitigating the risks posed by money laundering and terrorism financing. The use of a risk-based approach will allow licensees to focus resources on areas of greatest risks and the flexibility to respond to new risks as ML risks changes. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention.

Licensees are therefore obligated to assess the level of risks posed by ML/FT to their business and implement reasonable controls to mitigate such risk. All risk management policies must be reviewed by the Commission prior to implementation. The complexity of these policies and procedures will depend on the size of the operators business but must include the ***identification, categorisation, and mitigation of risks***.

Step 1 - *Identification of ML/FT Risks*

This is the first step in utilising a risk based approach. Licensees should identify any ML/FT risks facing their business with particular emphasis on the type of customers and the services being requested by such customers, and how the business itself is likely to be involved in ML.

The onus is on Licensees to review from time to time all available information on ML including: published money laundering typologies and terrorist lists; listed entity bulletins; notifications by the Supervisory Authorities (the Bank of Jamaica and the Financial Services Commission); notifications and directives of the Designated Authority (the Chief Technical Director of the Financial Investigations Division) and the Competent Authority (the Betting, Gaming and Lotteries Commission).

An effective AML/FT risk assessment of gaming lounges must take into account risks posed by customers as well as risks associated with the nature of the business itself. To effectively carry out a risk assessment of the gaming lounge, a number of questions must be addressed which may include but is not limited to:

Assessing risks posed by customers

- Who is the customer? Is there public information that associates this person with any money laundering or terrorism financing activity?

- What is the person's business? Is this customer's occupation or business activities commonly linked to or associated with money laundering or terrorism financing activities?

- Where is the person located or resident? Does the person's jurisdiction apply globally acceptable ML/FT standards?

- What services and/ or products does the person require? Do the services or products provided to the customer offer the movement of funds and anonymity usually linked to ML/FT activities

Assessing risks associated with the nature of the business

- Are customers generally well known and locally based?
- Is the business high volume or low volume or mixed?
- Are customers low spending or high spending, or mixed?
- Is there likely to be a situation where a customer cannot easily explain his source of fund?
- How is most business conducted? i.e. through customer accounts or some other contractual arrangements?
- Are customers likely to engage in transactions involving large amounts of cash?
- Are procedures in place to monitor customer transactions?

Step 2 – *Categorisation of Risk*

In order to detect suspicious activity, it is necessary to monitor customer transactions and/or activities. The risk based approach to monitoring customer transactions involves establishing ongoing customer due diligence and verification procedures and establishing a risk profile regarding all business relationships and one-off transactions with a view to determining which the ML risk posed. That is to say, customers, services and products provided by Licensees should be placed into two categories viz., Low Risk or High Risk.

Low Risk Indicators

These are customers, services and products that have a less than average chance of exposing a licensee to ML/FT.

Examples of such customers include:

- Customers who are employed/have a regular income from known source(s).

High Risk Indicators

These are customers, services and products that have a greater than average chance of exposing a licensee to ML/FT. (See Regulation 7A)

Examples of high risk customers include:

- Politically Exposed Persons;
- a person who is not ordinarily resident in Jamaica;
- a member of a class or category of persons specified by a Supervisory Authority and notification of which is published in the Gazette;
- a person acting as trustee;
- a company having nominee shareholders;
- a company having shares held in bearer form

A Politically Exposed Person is any individual who in relation to any State carries out functions analogous to any of the following:

i. a head of state;

ii. a head of government;

iii. a member of any House of Parliament;

iv. a Minister of Government;

v. A member of the judiciary;

vi. a military official above the rank of Captain;

vii. a member of the police of or above the rank of Assistant Commissioner;

viii. a Permanent Secretary, Chief Technical Director or chief officer in charge of the operations of a Ministry, department of Government, executive agency or statutory body;

ix. a director or chief executive of any company in which the Government owns a controlling interest;

x. an official of any political party;

xi. an individual who carries out any prominent function at the behest of an international organisation;

xii. an individual who is a relative or is known to be a close associate of any of the above.

"Close associate" means an individual who is a business partner, or associated in any other form, in a common commercial enterprise with the person concerned;

"Relative" means the person's spouse (legal and common law), child, step child, adopted child, spouse of child, parents, brother or sister.

Examples of high risk services and products include: (This is just an indicative listing and is not exhaustive)

- Facilities for large cash transactions, for example VIP/high roller service;
- person maintaining trading operations in known drug producing/transhipment locations;

Notably, higher risk customers should be subjected to greater scrutiny than low risk customers. Albeit, it does not mean that because a customer is assessed as having a higher risk of ML/FT, that person is involved in criminal activity; neither does it mean that customers assessed as posing a lower risk of exposing the business to ML/FT is definitely not involved in ML/FT.

Step 3 – Mitigation of Risk

Licensees are to take appropriate reasonable steps to mitigate against ML/FT risks.

PART THREE

THE COMMISSION'S APPROACH TO SUPERVISION

The Commission was established under the Betting, Gaming and Lotteries Act, to regulate and control the operation of betting and gaming and the conduct of lotteries in the island.

The Commission uses a risk-based regulatory regime, which underpins its licensing, compliance and enforcement functions. This ensures that focus is placed on those operators and issues where the impact of failure to deliver the licensing objectives would be highest. Thus, when conducting a compliance examination of licensees' policies and procedures, consideration will be given to the size, scope and complexity of the gaming lounge's activities.

The Commission's strategy for managing and mitigating identified ML/FT risks encompasses:

- prevention, through the provision of guidance, advice and information
- detection, through monitoring and assessment
- deterrence, through investigation and enforcement

ON-SITE EXAMINATIONS

The Commission as the Competent Authority is mandated to carry-out, either on its own behalf or through a third party, such inspections or verification procedures as may be necessary to evaluate and monitor the level of compliance of the businesses concerned. As such, the Commission will conduct on-site examinations of licensees AML/CFT policies throughout the examination year.

The on-site examination is not an audit of the business activities of the licensee but a procedure designed to determine, among other things, the adequacy and effectiveness of policies and procedures for the prevention and combating of ML/FT in accordance with the requirements under POCA and its regulations.

It shall be the responsibility of the licensee to pay the cost of all examinations whether conducted by the Commission or through a third party.

Examination Year

The examination year of the Competent Authority is from April 1 to March 31.

Types of Examinations

There are four types of on-site examinations which the Competent Authority may conduct. These are categorised as routine, follow-up, random, and special.

Examinations are carried out by the Compliance Division of the Competent Authority. They may also be conducted by, or with the assistance of a third party which has been duly appointed by the Competent Authority for such purpose.

Routine Examination

This is an annual on-site examination conducted by the Competent Authority geared towards testing and evaluating compliance with applicable AML/CFT laws by a licensee.

The law requires that internal controls are established and implemented and the examination focuses on seven (7) major operational areas of activities:

1) Procedures to ensure high standards of integrity of employees including a system to evaluate the personal employment and financial history of employees (employee due diligence policies and procedures)
2) Identification and verification of identification of customers (customer due diligence policies and procedures) including more rigorous requirements for high risk customers and transactions (enhanced due diligence policies and procedures)
3) Maintenance of records of identification/verification of identification, and unusual transactions
4) Appointment, role and responsibilities of the nominated officer (also referred to as the Compliance Officer)
5) Programme for training of employees in their responsibilities under the relevant laws
6) Schedule of independent audit to ensure programmes, policies, and procedures are being implemented
7) Reporting of suspicious transactions to the Designated Authority

Completed examination forms are discussed with the licensee. Where an adverse rating is received on a routine examination, a follow-up examination will be scheduled.
See Appendix 3: Notice of Intention to Conduct Routine Examination

Follow-up Examination

Follow-up examinations are for the purpose of addressing any deficiencies that are revealed through the routine examination process.

Where an adverse rating is given, the Commission will issue a notice advising of a follow-up examination to take place within ninety (90) days of the completion of the evaluation. However, where the deficiencies are of a grave nature, a notice will be issued advising of follow-up examination to take place within thirty (30) days.

In both instances, the notice advising of a follow-up examination will be issued within seven (7) days of the date on which the routine examination was conducted.

Random Examination

In addition to routine examinations, all licensees are subject to random examinations carried out by the Compliance Division of the Competent Authority.

The purpose of a random examination is to test the routine examination process and the process to be followed is the same as that for the routine examination.

Special Examination

The Competent Authority will conduct an examination of a licensee in special circumstances. Special circumstances may include, inter alia: consistent non-compliance with the law and/or procedures to ensure adherence with the law; information coming to the attention of the Competent Authority that a licensee is providing services having advised otherwise to the Competent Authority.

The special examination may take the form of a routine examination, or a specific investigation directed towards a specific issue or activity.

OFF-SITE EXAMINATIONS

The POCA (amendment) gives the Commission the authority to request licensees in writing to make reports in respect of such matters as may be prescribed in the notice. As such, periodic off-site monitoring will be conducted by the Commission through written requests for certain information, from time to time, from licensees regarding their compliance policy (and includes reviewing self audit reports of the licensees);

AUDITS

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

SELF-AUDITS

Licensees may wish to, and are encouraged to conduct (through the Nominated Officer) internal audits of their compliance policy from time to time to time to ensure their compliance with all applicable ML/FT laws, regulations and established policies, procedures and controls. Self audits provide the opportunity for licensees to review existing policies and practices, identify any weaknesses in their operations, and facilitate timely remedial actions.

PART FOUR

Customer Due Diligence (CDD)

It is very important for operators to know their customers; not only to verify compliance with age but also to mitigate the risks associated with the placement of tainted money within their businesses. Therefore, operators are obliged to develop and implement a customer due diligence policy (also known as know your customer (KYC) policy), which will detail reasonable procedures or steps to be taken for the identification of customers, the verification of that identification and the monitoring of their accounts. These procedures are outlined in Regulation 7 of the Proceeds of Crime (Money Laundering Prevention) Regulation and are necessary to ensure that licensees are satisfied that their customers are who they claim to be and that any funds associated with these customers are derived from legitimate sources.

CDD policies and procedures should include at a minimum:

- Customer acceptance criteria
- Identification of the direct customer
- Verification that the customer is, who he or she claims to be; and
- Ongoing due diligence and scrutiny of the customer's business as well as identity

Operators must establish to their satisfaction that they are dealing with legitimate persons (natural, corporate or legal) and verify the identity of those persons who have authority to conduct business.

Customer acceptance policy

A clear policy outlining explicitly the criteria for the acceptance of customers must be implemented as the law prohibits operators from ***forming a business relationship or one-off transaction*** with any person unless evidence of their identity have been provided by them and verified by the operator.[2]

Where the licensee's dealings with a customer are limited to a one-off transaction, and the customer is not establishing a business relationship, a risk assessment of that customer must still be done and if the employee suspects that the funds in the transaction is related to ML/FT, a suspicious transaction report must be made to the Designated Authority.

Customer identification process

Customer identification refers to the process whereby independent and reliable information is used as a means to identify the customer and then to verify his identity. Essentially, operators must be able to satisfy the Commission that proper steps were taken ascertain the identity of the customer. **See Appendix 4: Customer Identification Procedures**

[2] Regulations 6, 7 &11 AMLs

Verification procedures

Verifying a customer's identity consists of the operator checking some of the information provided by the customer against information obtained from a reliable and independent source. Where an operator is unable to verify a customer's identity, the law requires him to discontinue the transaction or the business relationship or in the case of a one-off transaction not to proceed any further (**Regulations 7 of the Proceeds of Crime (Money Laundering Prevention Regulations**).

Also, operators are required to implement a policy for the verification of transactions conducted within their businesses. This policy must be maintained in accordance with the Proceeds of Crime (Money Laundering Prevention) Regulations. As such, transaction verification procedures are only in accordance with the regulations where the steps taken in the verification procedure "produce satisfactory evidence as to the purpose and intended nature of the business relationship or one-off transaction..."[3]

Evidence will be considered to be satisfactory where it includes information pertaining to whether a transaction involves the prescribed amount, whether it is carried out in a single operation or in several operations, whether it is carried out by means of wire transfers, whether there is any doubt about the veracity or adequacy of previously obtained evidence of identity and whether the reporting entity (the operator) is required to make a report under section 94 or 95 of POCA.[4] Where such evidence has not been maintained, the business relationship or one-off transaction must not proceed any further.

A licensee should be aware that the best identification documents are those that are the most difficult to obtain illicitly. Positive identification should be obtained from documents issued by reputable sources such as the identification provided by governments.

The name and permanent address of a customer should be verified by an independent source, other than those provided by the customer. This must be done in accordance with the licensee's identification procedures. ***The following methods of verification are merely examples***:

- requesting sight of a current utility bill from the client's place of residence (that is, electricity, telephone, and water);
- checking a local telephone directory;

Whenever possible, the prospective customer should be interviewed.

Please note, that customer identification must be verified with transactions greater than three thousand United Stated Dollars or its equivalent in Jamaican or any other currency. However, transactions which fall below the prescribed amount do not need to be subjected to such processes, unless the nature of the transaction is such as to give rise to the knowledge or belief, or reasonable grounds for the knowledge or belief that the transaction constitutes or is

[3] Regulation 7 AML

[4] ibid

related to ML. **See Appendix 5: The Proceeds of Crime (Money Laundering Prevention Regulations) (De minimis amount) Order**.

Enhanced Due Diligence (EDD)

Enhanced Due Diligence procedures must be applied to High Risk categories. EDD procedures include:

- senior management approval to commence the business relationship (where applicable);
- verification of the source of funds or wealth held by the proposed client and others concerned in the business relationship or one-off transaction;
- enhanced monitoring throughout the course of the business relationship;
- more frequent updating of customer information;
- more detailed information as to the nature of the business relationship or one-off transaction;
- more detailed information about the prospective customer and other parties concerned in the transaction;
- selection of patterns of actions that require more detailed examination;
- requirement that the first payment in the transaction be carried through an account, in the name of the customer with a licensed and regulated financial institution; and
- identification and verification standards set out under customer due diligence requirements above.

The deminis amounts not requiring identification

As stated above, unless the nature of a transaction is such as to give rise to the knowledge or belief, or reasonable grounds for the knowledge or belief, that the transaction constitutes or is related to money laundering, the identification procedures set out in regulation 7 shall not be required in the case of customer transactions of a value of three thousand United States dollars ($3,000 USD) or its equivalent in any other currency or less.

PART FIVE

EMPLOYEE DUE DILIGENCE

It is a statutory requirement that policies and procedures be implemented to ensure the highest standard of integrity among employees of licensees, and that the personal employment and financial history of all employees is known and, or verified. Therefore, the hiring process for employees must include a background and employment history checks/verifications.

Under the Betting, Gaming and Lotteries Act, **ALL** persons employed in any prescribed premises who receive or negotiate bets on gaming machines or who are involved in the operation of the gaming machines on those prescribed premises, are required to obtain a 'Prescribed Premises Worker's Licence' from the Commission. As a part of the licensing procedure, such workers will be subjected to due diligence investigations carried out by the Commission. ***This will help to ensure the integrity of employees, thereby aiding licensees with employee due diligence***.

There must be continuous monitoring of employees to ascertain, inter alia:

- Lifestyle changes and reasons for same
- Unusual transaction activities
- Inappropriate client relationships
- Association with persons known to be involved in criminal activities
- Refusal to take holidays

Training

Licensees must make provision for training of ALL relevant employees. Relevant employees are those persons employed in any prescribed premises who receive or negotiate bets on gaming machines or who is involved in the operation of the gaming machines on those prescribed premises. This includes front-line customer-contact employees, line operations staff, senior management and directors. The policy for training employees in ML/FT matters must be in writing, must be updated regularly and reviewed annually to test their effectiveness. Documentation of training and the identity of the employees trained must be retained.

Employees must be made aware (example, staff training to ensure that they obtain CDD information and reporting of suspicious transaction) on a continuous basis of:

- provisions of the law pertaining to money laundering and the financing of terrorism;
- procedures for the recognising and handling suspicious transactions;
- reporting procedures;
- their personal liability under the law for failure to report and tipping-off; and
- procedures for internal control and communication.

The Commission will organise training programmes for licensees and their employees twice per year at a cost to the licensees. Also, officers of the Commission will be available for specific training programmes for individual gaming lounges upon request.

It is imperative that employees are required to adhere to a Code of Conduct which sets out minimum standards of behaviour expected of employees and they should be required, on an annual basis to acknowledge that the Code has been read and understood, and that breach of the Code may result in dismissal from employment and criminal sanctions in some cases. New employees must receive training related to the business's AML/CFT compliance policy prior to handling customer transactions.

Further, all operators are to inform the Commission, in writing, of the identity of the nominated officer. If at any time, such persons shall cease to operate in that capacity, the Commission must be notified.

PART SIX

RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS

The Financial Investigations Division

The Financial Investigations Division of the Ministry of Finance & Planning is an authority established under the Financial Investigations Division Act, 2010 to investigate all categories of financial crimes including money laundering and the financing of terrorism. The Division is empowered to collect, request, receive, process, analyse and interpret information relating to financial crimes and transaction reports and other reports made to, or received by the Division under the Act or any other enactment.

The head of the Division is the Chief Technical Director who is the Designated Authority under POCA and TPA.

DNFIs submit reports to, and receive directives from the Chief Technical Director.

The Nominated Officer

DNFIs are required to appoint an officer of the business who performs management functions as the Nominated Officer. The nominated officer will be responsible for ensuring the implementation of AML/CFT programmes, policies, procedures and controls, and reporting of suspicious transactions.

The Nominated Officer is the point of contact with the Designated Authority.

The type of person appointed will depend on the size and nature of a licensee's business. Larger licensees/firms may choose to appoint a senior member of their compliance, internal audit or fraud departments. In the case of an individual licensee or small licensees/firms, it may be appropriate to appoint as the case may be, the sole licensee or the office administrator. When several licensees operate closely together within a group, a Nominated Officer at group level should be appointed.

The roles and responsibilities of the Nominated Officer must include:

- Coordination and monitoring of day-to-day compliance with applicable AML/CFT laws and regulations and internal AML/CFT policies and procedures ;
- Conducting and/or coordinating scheduled employee training programmes and on-going trainings for personnel related to the licensees' AML/CFT policies and procedures and maintaining and reviewing records evidencing such training;
- Responsibility for training newly recruited employees immediately upon assuming employment ;
- Observing and ensuring implementation of internal controls and procedures;
- Receiving and reviewing any reports of suspicious activity from employees regarding suspected money laundering;[s. 94 (3)]
- Reporting of all suspicious activity as reported by an employee to the Designated Authority;

- Responsibility for ensuring the reporting of suspicious transaction reports to the Designated Authority;
- Coordination of the annual audit of the AML/CFT programme;
- Coordination of enhanced due diligence procedures regarding high risk clients;
- Responding to both internal and external inquiries regarding AML/CFT policies and procedures;
- Ensure periodic reviews are carried out to identify unusual activities
- Provide reports to senior person(s) on AML/CFT issues affecting the licensee;
- Overall responsibility for the supervision of Record Retention requirements.
- Responsibility for ensuring that recommendations from any examinations by the Competent Authority and any External Audit are promptly reported to the relevant internal body for review and once approved, are implemented.

The Nominated Officer is required to determine whether the information or matters contained in a suspicious transaction report give rise to a knowledge, suspicion, or belief that a client is engaged in money laundering. In arriving at a judgment, the Nominated Officer must consider all other relevant information which is available including transaction patterns, volume of funds and assets, length of the business relationship, and identification and transaction verification records.

The Nominated Officer can be held personally liable for failure to report or for giving consent to the carrying out of a transaction which has been reported to the Designated Authority and for which the required procedures and time frames have not been met.

Recognition of Suspicious Transactions

'Knowledge', 'reasonable grounds for belief (suspicion)' and 'complex, unusual and large business transactions'

POCA makes reference to knowledge, suspicion and complex, unusual and large transactions. Businesses in the regulated sector are required to make 'required disclosures' where there exists knowledge or a suspicion that the transaction involves the proceeds of crime. Knowledge in the context of POCA means actual knowledge. That is, actually knowing for a fact that the customer is involved in or engaged in criminal activity.

A suspicion on the other hand usually involves a belief that the possibility exists that the transaction involves criminal property. This belief, however, must go beyond mere speculation. An employee may notice activity which is unusual or inconsistent with the customer's known legitimate business or personal activities or with normal business activities for that type of transaction and having made some enquiry, obtains a degree of satisfaction which is more than just a gut feeling that the relevant fact exists; this may amount to a suspicion and a Suspicious Transaction Report must be filed. If, however, the suspicion is favourably resolved, reasons for not reporting must be documented and retained.

Customer due diligence procedures will oftentimes assist in determining whether the customer's activities or proposed activities are of an unusual nature thereby giving rise to suspicions.

Some examples of suspicious activities are:

- The purchasing of tokens/chits, or crediting accounts, with cash and then redeeming their value by way of bank drafts, cheque or other non-cash instrument;
- The purchase of large value of tokens/chits with cash, playing an insignificant amount and then redeeming the value by way of non-cash instruments;
- The presence of a third party for all transaction who does not participate in the actual transaction;
- High volume of transaction within a short period;
- Customer attempting to befriend an employee;
- Customer requested to add cash to winnings and then exchanging cash and winnings for a single cheque;
- Use of multiple names to conduct transactions;
- Use of multiple debit cards to purchase tokens;
- an individual who was recently released from prison and is unemployed and starts to gambling large sums of money;
- a person is known to be involved in illegal activities, is unemployed and gambles large sums of money;
- Exchanges of small denomination cash for bills of larger denomination; and
- Accumulating excessive credits on gaming machines by constantly adding cash and then cashing out to obtain large denomination bills.

Where knowledge or reasonable grounds for belief that a transaction involves the proceeds of a criminal activity, a required disclosure must be made to the Designated Authority immediately by the nominated officer. Accordingly, employees should know to whom (nominated officer) reports of suspicions are to be made and the format in which such reports should be made.

However, it is important to note that a distinction is made by POCA between suspicious transactions and unusual transactions. Complex, unusual or large business transactions do not require a report to the Designated Authority; instead, licensees are asked to pay special attention to these transactions and keep a record of them. Such records must be kept for a period of seven (7) years (s. 94).

Unusual or complex transactions therefore, should not necessarily lead to knowledge or suspicion of ML/terrorism financing.

Recording and Reporting Financial and Suspicious Transactions

Licensees are required to keep a general record of all transactions, as well as records attributable to each player. As such, monitoring of transactions or activities may be done in real time or afterwards. Real time monitoring involves monitoring of transactions or activities as they take place. An account must be taken of the frequency and the size of customers transactions. The complexity of this monitoring will depend on the size of the operator's business but a common feature should be that customers' information is current.

Internal Reports

Reporting Suspicious Transaction

Employees of a gaming lounge operator are legally obligated to make reports (required disclosures/STRs) of activities or transactions to their nominated officer, where they suspect or have knowledge that such activity involves the proceeds of crime[5]. Where this is done, the employee is afforded a legal defence against prosecution for engaging in or dealing with criminal proceeds.

Again, it is important to point out that operators must provide training for employees so that they can obtain the relevant knowledge to insure compliance with the POCA and its regulation.

All internal reports to the nominated officer must be considered by the nominated officer for a determination as to whether in light of all relevant information the report leads him to form a knowledge or suspicion or to have reasonable grounds for knowledge or suspicion that the transaction involves the proceeds of crime. Therefore, reports by employees to their nominated officers are required to be made as soon as is **reasonably practicable** and in any event within **fifteen (15) days** after receiving the information.

External Reports

There is no statutory threshold transaction reporting requirements for DNFIs. However, there are two (2) types of report that licensees are required to submit under POCA. These are: -

- Suspicious Transaction Reports (STR); and
- Authorised Disclosure and Request for Consent

Reporting Suspicious Transactions

The nominated officer is required to report all suspicious transactions to the Designated Authority. POCA refers to Suspicious Transaction Reports as "required disclosures".

Licensees are required to make the required disclosure (STR) to the Designated Authority, if:

(a) that person knows or believes, or has reasonable grounds for knowing or believing, that another person has engaged in a transaction that could constitute or be related to money laundering; (Section 94, 2a)

(b) the information or matter on which the knowledge or belief is based or which gives reasonable grounds for such knowledge or belief, came to him in the course of a business in the regulated sector. (Section 94, 2b)

[5] S.94 (3) POCA amendment

Similarly, Licensees are required to submit to the Designated Authority, all transactions, whether completed or not, which it suspects or has reasonable cause to suspect:

- involve property connected with, or intended to be used in, the commission of a terrorist offence or
- involve, or are for the benefit of, any listed entity or terrorist group.

Procedures for Reporting Suspicious Transactions to the Designated Authority

This report must be made in the prescribed form: Form I – POCA

Unique Reference Number

Each report must be assigned a unique reference number. The format should be YYYYMMDD/ABC/00001 representing:

YYYYMMDD	Date of the report
ABC	An acronym for the reporting institution
00001	Consecutive numbering of reports submitted. First report for the year should end with the number 00001; succeeding reports assigned consecutive numbers 00002, 00003 etc.

For reports submitted under Terrorism Prevention Act add TPA at the end of the number, for instance YYYYMMDD/ABC/00001/TPA. TPA reports must have their own numbering sequence.

Each Licensee falling within a corporate group should make separate and independent reports.

Cover Letter

A cover letter on the reporting entity's letterhead listing the reports being forwarded to the DA should accompany all submissions of reports. For large submissions a summary sheet can be attached to the cover letter by way of an appendix.

The cover letter should be submitted in duplicate, requesting that the copy be signed and returned as acknowledgement of receipt. The cover letter should indicate the reporting period and the number of reports being submitted.

The cover letter or summary sheet should also provide the following information:

- Name of customer
- Date of transaction
- Transaction Amount
- Unique Reference Number

Acknowledged cover letters should be retained by the reporting entity as proof of submission for their regulator's inspection.

Suspicious transactions are to be reported **promptly** and in any event within **fifteen (15) days** after the suspicion or reasonable cause for suspicion arises. Such reports are to be sent to:

The Designated Authority
The Chief Technical Director
Financial Investigations Division,
Ministry of Finance and Planning,
1 Shalimar Avenue,
Kingston 3.

Note: All the information necessary to complete the STR will not be available in all instances; nevertheless, the STR should still be submitted to the DA with whatever information is available. An example of an instance in which all relevant information may not be available is where a licensee requests identifying information and the customer leaves the premises immediately.

Request for additional information

Under regulation 3(6) of POCA, the Designated Authority can direct a licensee that has filed a suspicious transaction report to provide information as to:

- Previous or current reports,
- The provision of information required in such reports, and
- The provision of additional information in relation to queries in relation to queries concerning specific matters arising from the reports, including:
    - Due diligence procedures followed in relation to a specific transaction
    - Persons authorized to sign on the account in question
    - Errors identified in the reports, and
    - Such other matters as may be specified in the directions.

Authorised Disclosures and Appropriate Consent

A person in the regulated sector commits a money laundering offence where he handles or engages in a transaction that involves the proceeds of crime. However, if before doing so, he makes a report to an authorised officer of the FID or a nominated officer (authorised disclosure) seeking consent to do so and receives the 'go ahead' (appropriate consent), this may be used as a defence. Similarly, if such a report is made after the transaction has taken place but the person had a reasonable excuse for not reporting it before, and reports it as soon as is reasonable practicable, a defence in law exists. What amounts to a reasonable excuse will be determined by the courts.

Appropriate Consent

Where grounds for knowledge or belief exists that a transaction involves the proceeds of crime/ criminal property, the consent of the FID must be sought before proceeding with the transaction.

By virtue of section 91 (2) (b), a person shall be deemed to have the appropriate consent if the person makes an authorized disclosure to an authorized officer and-

(i) before the end of the notice period the person is not notified by the authorized officer that consent to the doing of the act is refused; or
(ii) the person is so notified before the end of the notice period, but ten days have passed since the receipt of the notice.

The notice period referred to in section 91 (2) (b) is the period of seven days (exclusive of Saturdays, Sundays and public general holidays), starting with the first day after the person makes the disclosure.

Procedure for seeking appropriate consent

Consent should be requested through the completion and submission of an authorized disclosure (Form 111), to the FID. **See Appendix 6: FID Advisory to DNFI**

Prohibitions on financial transactions

Limits on cash transactions

A person cannot–

1. Pay or receive cash in excess of the prescribed amount in a transaction for the purchase of any goods or services or for payment or reduction of any indebtedness, accounts payable or financial obligation; or
2. Artificially separate a single activity or course of activities into a set of transactions so that each transaction involves a payment and receipt of cash that is less than the prescribed amount but which activity or course of activities in aggregate involves payment and receipt of cash that exceeds the prescribed amount. [section 101A]

This therefore means that operators are not to accept bets or wagers in ***cash*** for over one million dollars ($1,000,000), nor make a payout (of winnings) in ***cash*** of the said amount; neither can the cash transaction be separated so as to accept/receive the prohibited amounts in more than one part.

What is a single activity/transaction?

A single transaction/activity is generally considered to be any financial event which takes place at one time. Examples include, a deposit to or withdrawal from a credit or safekeeping account, any single bet or wager, or single payout such as a jackpot; and cashing a cheque for a payout request; and wire transfers.

POWER POINTS:

Licensees:

1. The FID is authorised to investigate all categories of financial crime
2. DNFI are obligated to appoint a nominated officer – who will be responsible for monitoring the business' compliance with POCA and its regulation in its day to day operations and make the required disclosures to the DA.
3. Must implement measures to identify suspicious transaction;

4. Employees must report all suspicious transactions to the nominated officer

5. All complex, unusual or large business transactions must be recorded and the record kept for at least seven (7) years.

6. All cash transactions in excess of one million dollars ($1,000,000) are prohibited

7. Licensees are prohibited from artificially separating a single activity or course of activities into a set of transactions so that each transaction involves a payment and receipt of cash that is less than the prescribed amount.

PART SEVEN

RECORD KEEPING

Statutory Requirements to Maintain Records

The maintenance of records is an important tool in the provision of evidence in investigations and a critical method of following an audit trail.

A licensee is required to retain records of identification, verification of identification documentation, and records of transactions for a minimum period of at least seven years. The retention period commences on the date of the last transaction or on the date that the customer file is closed, whichever is later.

Records which are maintained should wherever possible be original documentation or reproductions of the original documentation. The customer file should indicate, where necessary, the location of the original documentation.

Retention of records may be by way of original documents, microfiche, computer disc or other electronic form.

Records of customer relationships and transactions should be such that:

- Requirements of legislation are fully met;
- Competent third parties will be able to assess observance of money laundering policies and procedures;
- Any transaction which has been carried out can be reconstructed; and
- Retrieval can be effected within a reasonable time to satisfy enquiries and court orders.

Where records relate to on-going investigations, they must be retained until it is confirmed by the Designated Authority or any other law enforcement agency that the case has been closed.

Records need not be kept where a client, being a company has been liquidated and finally dissolved or, being a partnership, the partnership has been legally dissolved.

As it concerns any business relationship, a customer's information is to be **updated at least once in every five years** during the course of the business relationship and whenever there is doubt about the veracity or adequacy of previously obtained customer information. Failure to update the information as required will result in the business relationship being halted.[6]

Records must be kept of contact or communication between the licensees business and the Designated Authority and the Commission, including records connected to:

- Appropriate consent;
- External suspicious transaction reports

Additionally, detailed records of employees training and internal suspicious transaction report must be kept. **Records must be kept for a minimum period of 7 years**.

[6] Regulation 7 AML

PART EIGHT

Tipping Off

Under section 97 (1) of POCA, a person commits an offence if knowing or having reasonable grounds to believe that a disclosure has been made or 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 the information, which is likely to prejudice any investigations, to any other person. Once an operator or any person within his employ knows or suspects that a disclosure has been made this must be kept confidential and not shared with any other person.

The tipping off offence is a serious offence and operators are to be aware of the provisions, as the penalties are a fine of 1 million dollars, imprisonment or both a fine and imprisonment. Further, there are a number of defences that may be available such as that the disclosure was made to an attorney-at-law for the purpose of obtaining legal advice or at the time of making the disclosure, the person did not know or suspect that it was likely to be prejudicial.

APPENDIX 3: Notice of Intent to carry out Routine Examination

Routine Inspection Confirmation Letter to Gaming Lounges (Example)

For announced inspections ONLY, i.e. for routine examinations, the Senior Inspection team leader should send this letter/Notice to ALL Gaming Lounges to be inspected.

(The team leader should also place a copy of this letter, once it is customized, in the Audit & Compliance Folder on the shared drive)

Dear _____:

This letter is to confirm our telephone conversation in which we arranged the Anti-Money Laundering routine examination of your operations. We plan to arrive at your location on (...) at about (...) and anticipate that the routine examination will last approximately (...) days.

The team will comprise of: (Name of inspector)

We would like to meet with you and your nominated officer briefly at the beginning of the visit to review the general expectations and documentation required.

We intend to complete the examination by (...), at which time we would like to meet with you and your staff again for the exit conference.

Sincerely,

BETTING, GAMING & LOTTERIES COMMISSION

_____

Team Leader's Name

APPENDIX 4:

Customer Identification Procedures for Natural Persons

A licensee must take reasonable steps to ascertain satisfactory evidence of an individual client's:

- true name and names used / Alias;
- current permanent address, including postal address;
- date and place of birth;
- nationality;
- occupation, including the employer's address;
- Tax Registration Number; and
- source of funds.
- Recent photograph

Identification of Natural Persons Resident Overseas

The identification requirements for natural persons resident in Jamaica also apply to natural persons resident outside of Jamaica. A licensee is required to obtain the same identification documentation or their equivalents for a prospective customer resident outside of Jamaica.

Customer Identification Procedures for Bodies Corporate

A licensee must be vigilant when dealing with corporate vehicles as they may be used as a method of ensuring anonymity. In all cases a licensee must understand the structure of the organisation, the source of funds and the owners and/or persons with effective control of the entity.

A licensee must obtain the following documents or their equivalents in respect of new customers which are companies, other bodies corporate, or partnerships formed in Jamaica.

- Certificate of Incorporation or certificate of registration;
- Articles of Incorporation, Partnership Deed (whichever is applicable);
- A description of the customer's principal line of business;
- List of name and address of principal owners, directors, and beneficiaries;
- Group/Corporate structure, where applicable.

Identification of Overseas Bodies Corporate

The requirements for customer due diligence for domestic corporate customers are also applicable to overseas corporate bodies with which a licensee proposes to carry out business. Comparable documents to those listed above should be obtained for companies or any bodies corporate, partnerships, or trusts established outside of Jamaica.

Particular attention should be paid to the place of origin of such documents, and the background against which they are produced, bearing in mind that standards of control vary between countries. A licensee may obtain certified copies of documents, notarised by a foreign official, such as a notary public, or county clerk.

A licensee should also seek to determine and document the source of funds being used for any proposed transaction).

Identification of Principal and Agent

An agent is a person who acts for and on behalf of a principal. Where a person appears to be an agent, or is acting on behalf of another person, or on behalf of a body corporate or other legal arrangement such as a trust or settlement, a licensee must take reasonable measures to establish the identity of the principal, the agent, each beneficiary, and the ultimate beneficial owner of the property or funds pertaining to the proposed business transaction.

In these circumstances, a licensee must seek verification that the agent is authorised to act on behalf of the principal. Verification may include providing the licensee with documentation of appointment such as a Power of Attorney or Trust Deed.

A licensee may, in the following circumstance, accept a written assurance from an agent that evidence of the identity of the principal has been obtained and recorded in keeping with procedures maintained by the agent:

i. where the agent is based or incorporated or formed under the laws of a country in which there are equivalent anti-money laws and requirements in force; and

ii. the agent would be a regulated business if situated in Jamaica; and

iii. acts in the course of a business over which a foreign regulatory authority exercises regulatory functions and control.

Identification In The Case Of A Settlement, Trust Or Other Type Of Legal Arrangement

Where a licensee is proposing to enter into any transaction involving a settlement, trust or other type of legal arrangement, the licensee must be satisfied that:

- the identity has been established of (as the case may require) the settlor, legal owner or other person who exercises effective control of the legal arrangement, and each beneficiary under the legal arrangement, including the ultimate beneficial owners of the property concerned in the arrangement; and

- the legal status of the arrangement and the provisions regulating the power to bind the parties involved has been disclosed

APPENDIX 7:

Schedule of offences under the Proceeds of Crime Act

Table 1 shows a list of possible offences that a licensee may be charged with and the corresponding penalties.

Offence	**Section**	**Penalty - RM Court**		**Penalty-Circuit Court**	
		Individual	**Body Corporate**	**Individual**	**Body Corporate**
Concealing, transferring, converting etc, criminal property	92	Fine up to $3M and/or up to 5 yrs imprisonment	Fine up to $5M	Fine and/or up to 20 yrs imprisonment	Fine
Engaging in transaction that involves criminal property	92	Same as above	Same as above	Same as above	Same as above
Acquisition use and possession of criminal property	93	Same as above	Same as above	Same as above	Same as above
Non-Disclosure by a nominated officerin the regulated	94	Fine up to $1M and/or up to 12 months imprisonment	N/A	Fine and/or up to 10 yrs imprisonment	N/A
Tipping off	97	Fine up to $1M and/or up to 12 months imprisonment	N/A	Fine and/or up to 10 yrs imprisonment	N/A
Breach of appropriate consent provision by nominated officer	99	Fine up to $1M and/or up to 12 months imprisonment	N/A	Fine and/or up to 5 yrs imprisonment	N/A
Limit on cash transactions	101A	Fine up to $3M and/or up to 3 years imprisonment	N/A	Fine and/or up to 10 yrs imprisonment	N/A
Offences prejudicing investigation	104	Fine up to $1M and/or sup to 12 months imprisonment	N/A	Fine and/or up to 10 yrs imprisonment	Same as above
Failure to comply with the requirements of a disclosure order	112(1)	Fine up to $1M and/or up to 12 months imprisonment	N/A	N/A	N/A

Offence	Section	Penalty - RM Court		Penalty-Circuit Court	
		Individual	**Body Corporate**	**Individual**	**Body Corporate**
Makes a false or misleading statement with respect to a disclosure order	112(3)	Fine up to $1M and/or up to 12 months imprisonment	N/A	Fine and/or up to 5 yrs imprisonment	N/A
Failure to comply with the requirements of a customer information order	122(1)	N/A	Fine up to $1M	N/A	N/A
Makes a false or misleading statement with respect to a customer information order	122(3)	N/A	Fine up to $1M	N/A	N/A
Failure to comply with directions from DA & in provision of additional information	MLP Reg. 3(7)	N/A	Fine up to $400, 000	N/A	N/A
Failure to implement regulatory controls by regulated businesses	MLP Reg. 5(5)	N/A	Fine up to $400, 000	N/A	N/A
Failure to implement systems & training to prevent money laundering	MLP Reg. 6(2)	Fine up to $1M and/or up to 12 months imprisonment	Fine up to $3M	Fine and/or up to 20 yrs imprisonment	Fine
Breach of electronic funds transfers requirements	MLP Reg. 9(3)	Fine up to $1M and/or up to 12 months imprisonment	Fine up to $3M	N/A	N/A

APPENDIX 8:

Guide to Structuring an AML/CFT Compliance Policy

An effective compliance policy must contain policies and procedures for preventing, detecting and addressing non-compliance. Common features of an effective compliance policy must include, but are not limited to the following:

1. The appointment of a nominated officer;
2. The development and implementation of internal policies and procedure;
3. An assessment and documentation of money laundering related risks (and terrorist financing) and mitigation measures to deal with those risks;
4. Training for employees
5. A review of compliance policies to test their effectiveness.

Compliance policy manual should include:

1. Table of contents
2. A policy statement
3. Risk based approach
4. Internal policies procedures and controls which describes the who, what, why, when and how of the programme
5. Designation of a nominated officer
6. Internal procedures for employees to make reports to the nominated officer
7. Record keeping procedures
8. Review of the policy.