GUIDELINES ON THE PREVENTION OF MONEY LAUNDERING AND COMBATTING THE FINANCING OF TERRORISM FOR CASINO AND GAMING HOUSE "A" OPERATORS

Issued under Section 7 (1) (d) & 97A of the Gambling Regulatory Authority Act 2007 and Section 19H (1)(a) of the Financial Intelligence and Anti-Money Laundering Act 2002

MAY 2020

[Updated on July 2020]

The Guidelines on the Prevention of Money Laundering and Terrorist Financing was approved by the Board of the GRA on 27 May 2020.
This Guideline was issued on 29 May 2020 and comes in force on the same day.

DISCLAIMER

These Guidelines are intended to provide assistance to Casinos and Gaming Houses in meeting their obligations under the Gambling Regulatory Authority (GRA) Act 2007, the Financial Intelligence and Anti Money Laundering Act (FIAMLA), United Nations (Financial Prohibitions, Travel Ban and Arms Embargo) Sanctions Act 2019 (UN Sanctions Act) and the Financial Intelligence and Anti Money Laundering Regulations 2018 (FIAML Regulations).

These Guidelines have been issued by the GRA pursuant Sections 7(1) (d) and Section 97A of the Gambling Regulatory Authority Act 2007 and to Section 19H (1) (a) of the Financial Intelligence and Anti-Money Laundering Act 2002. This Guide has been prepared and published for informational and educational purposes only and should not be construed as legal advice. The laws and regulations discussed in this Guide are complex and subject to frequent change. If you are unsure about your obligations in a given case, you should consider taking independent legal advice.

The Guidelines must be read in conjunction with the Gambling Regulatory Authority (GRA) Act 2007, the Financial Intelligence and Anti-Money Laundering Act 2002, Prevention of Corruption Act 2002, Prevention of Terrorism Act 2002, the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, the Convention of the Suppression of the Financing of Terrorism Act and the Financial Intelligence and Anti-Money Laundering Regulations 2018.

These Guidelines shall be subject to subsequent amendments by the GRA as and when required by law. Stakeholders are urged to ensure that they consult the most up to date version.

TABLE OF CONTENTS

1. Introduction 1
   1.1 Purpose and Scope of these Guidelines 1
   1.2 Compliance with Guidelines and Enforcement 3
   1.3 What is ML/TF? 4
2. Background Information 6
   2.1 The Financial Action Task Force 6
   2.2 Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 6
   2.3 AML/CFT Conventions ratified by Mauritius 8
3. The Risk Based Approach 9
   3.1 Risk management is a dynamic tool 9
   3.2 Risk Categories 10
      3.2.1 Geographical risk 10
      3.2.2 Customer risk 11
      3.2.3 Transaction risks 13
      3.2.4 Product and Service risk 15
4. Governance Framework 18
   4.1 The Money Laundering Reporting Officer (MLRO) 19
   4.2 Deputy Money Laundering Reporting Officer (DMLRO) 20
   4.3 Compliance Officer(s) 20
   4.4 Screening of Employees and Third Parties 22
   4.5 Audit Function 23
   4.6 Training 23
   4.7 Policies, Procedures, and Controls 26
5. Customer Due Diligence (CDD) 29
   5.1 Introduction 29
   5.2 Thresholds 29
   5.3 Customer Due Diligence (CDD) Measures 32
      5.3.1 Identification 32
      5.3.2 Verification 32
      5.3.3 Third Party Agents 33
   5.4 Enhanced Due Diligence (EDD) 34
   5.5 Politically Exposed Persons (PEPs) 36
6. Suspicious Transaction Reporting (STR) 39
   6.1 Lodging a suspicious transaction report 40
   6.2 Request for Information by the FIU 41
   6.3 Disclosure of Information 42

6.4 Tipping off....42
6.5 Requirements to cease transactions or terminate relationship....43
7. Terrorist Financing Offences and Sanction Screening....44
7.1 Introduction....44
7.2 Extension of obligations....44
7.2.1 Reporting obligations....44
7.2.2 Reporting of suspicious information....45
7.2.3 Internal controls....45
7.3 Sanction Screening....45
7.3.1 Reporting Obligations....46
8. Nature and Scope of the Powers of a Regulatory Body under the FIAMLA....47
8.1 Nature of the power....47
8.2 Functions of the Regulatory Body....47
8.3 Scope of the powers of a Regulatory Body....47
8.4 Request for information....48
8.5 Onsite Inspections....49
8.6 Directions by Regulatory Body....49
8.7 Administrative sanctions....50
8.8 Compounding of offences....50
8.9 Review Panel....50

GLOSSARY

NRA	National Risk Assessment
FIAMLA	Financial Intelligence and Anti Money Laundering Act
GRA	Gambling Regulatory Authority
AML	Anti-Money Laundering
CFT	Combatting Financing of Terrorism
CDD	Customer Due Diligence
FATF	Financial Action Task Force
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
MER	Mutual Evaluation Report
POCA	Prevention Of Corruption Act
POTA	Prevention Of Terrorism Act
UN	United Nations
DNFBPs	Designated Non-Financial Businesses and Professions
FIs	Financial Institutions
DPP	Director of Public Prosecutions
PEP	Politically Exposed Person
VIP	Very Important Person
KYC	Know Your Customer
MLRO	Money Laundering Reporting Officer
AMLRO	Alternate Money Laundering Reporting Officer
STR	Suspicious Transaction Report
FIU	Financial Intelligence Unit
OFAC	Office of Foreign Assets Control
OECD	Organisation for Economic Co-operation and Development
IMF	International Monetary Fund

1. INTRODUCTION

1.1 Purpose and Scope of these Guidelines

The National Risk Assessment (NRA) on ML/TF of Mauritius which was issued in August 2019, demonstrated the high residual risk exposure of money laundering in the gambling sector given the nature of the industry which is cash-intensive ,thus making it vulnerable to be exploited by criminals seeking to launder ill-gotten gains. Since 2002, gambling and gaming operators have become subject person as per the Financial Intelligence and Anti Money Laundering Act (FIAMLA) 2002, thus it is expected that the sector adheres to the obligations contained in this document and other instruments pertinent to AML/CFT.

This Guideline has been issued pursuant to section 19H (1) (a) of the Financial Intelligence and Anti Money Laundering Act (FIAMLA) 2002 and section 7(1) (d) of the Gambling Regulatory Authority (GRA) Act 2007 which is intended to assist gambling businesses including both casino and gaming house A operators in complying with their obligations in relation to the prevention, detection and reporting of money laundering and the financing of terrorism and proliferation, through the implementation of these guidelines which delineate how casino and gaming house A operators are expected to mitigate these identified risks.

The Financial Intelligence and Anti-Money Laundering Regulations 2018 also govern casinos and gaming houses.

As per FIAMLA 2002, all gambling operators have the responsibility to detect and to the best of their capabilities, keep financial crime out of the gambling industry. For the avoidance of doubt, the FIAMLA 2002 places an obligation on gambling operators to monitor and report customer suspected to be performing activity with money acquired unlawfully, either to obtain legitimate or 'clean' money in return (and, in doing so, attempting to disguise the criminal source of the funds) or simply using criminal proceeds to fund their gambling tendencies which both circumstances are to be considered as money laundering.

The purpose of this guidance is to outline the legal framework for AML and CFT requirements and systems across casino and gaming house A operators;

- outline the requirements of the relevant AML/CFT laws and regulations, and how these can be implemented in practice;
- recommend industry practices on AML/CFT procedures with a particular focus on the risk-based approach;
- assist casino and gaming house A operators to design and implement their AML/CFT policies, procedures and the necessary controls to mitigate ML/TF risks;
- guide the industry with the Identification, Due Diligence and Verification of customers;
- highlight industry practices with Record Keeping procedures;
- setting AML/CFT training expectations of stakeholders within the gambling sector; and
- the provision of expectations with suspicious transaction reporting with the FIU.

Whilst this guidance sets out what is expected of casino and gaming house A operators in terms of AML/CFT obligations, it is understood that not each and every subject entity has the same ML/TF exposures and thus to a certain degree, these exposures shall vary from one business to another. In view of this, casino and gaming house A operators are expected to perform their individual AML/CFT Business Risk Assessment in order to identify their relevant ML/TF risks which shall then allow for a better application of these proposed mechanisms and in proportion to the entities' residual exposures. This approach is better referred to as a 'Risk-Based Approach'.

Furthermore, whilst this guidance focuses primarily on the relationship between casino and gaming house operators and their respective customers, operators should also give due consideration to the ML/TF risks posed by their business associates, including any third parties they contract with.

1.2 Compliance with Guidelines and Enforcement

According to section 7(1)(j) of the GRA Act, the GRA may impose any financial penalty for non-compliance with these guidelines.

According to section 7(1 (ma) of the GRA Act, the GRA must ensure that licensees comply with the relevant guidelines issued by the FIU under the Financial Intelligence and Anti-Money Laundering Act.

According to section 97A of the GRA Act, every licensee shall comply with the relevant guidelines issued by the FIU under the FIAMLA.

According to section 99 (ka) of the GRA Act, the Board of the GRA may, at any time, refuse to renew, or suspend for such period as the Board may determine, or revoke or cancel from such date as the Board may determine, any licence where the licensee fails to comply with the relevant guidelines issued by the FIU under the FIAMLA.

According to section 139 of the GRA Act, any person who fails to comply with guidelines issued under the GRA Act shall commit an offence and shall, on conviction, be liable to a fine not exceeding 100,000 rupees and to imprisonment for a term not exceeding one year.

According to section 33 of the Financial Intelligence and Anti-Money Laundering Regulations 2018, any person who contravenes these regulations shall commit an offence and shall on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

Failure to comply with the minimum requirements of the FIAMLA, FIAML Regulations and the guidelines may result in regulatory action and be regarded by the GRA as an indication of:

(a) conduct that is not in the best economic interests, or which damages the reputation of Mauritius; and/or

(b) lack of fitness and propriety.

1.3 What is ML/TF?

Money laundering is generally defined as the process by which the proceeds of crime, and the true ownership of those proceeds, are changed so that the proceeds appear to come from a legitimate source. Under section 3 of the FIAMLA, the definition is broader as it puts an added layers of obligation on members of a relevant profession and occupation to prevent its services from being used to launder illicit funds or otherwise the financing of terrorism whilst also captures the elements of conspiracy under section 4 of the FIAMLA.

There are three and distinct phases to money laundering, namely:

- placement,
- layering
- integration.

Placement is the first stage in the money laundering cycle. The laundering of criminal proceeds is often required because of the cash-intensive nature of the underlying crime (for example, drug dealing where payments are typically in cash and often in small denominations). The monies are placed into the financial system or retail market, or are smuggled to another country. The aim of the money launderer is to avoid detection by the authorities and to then transform the criminal proceeds into other assets.

Layering is the next stage and is an attempt to conceal or disguise the source and ownership of the criminal proceeds by creating complex layers of financial transactions which obscure the audit trail and provide anonymity. The purpose of layering is to disassociate the criminal proceeds from the criminal activity which generated them. Typically, layers are created by moving monies in and out of various accounts and using electronic fund transfers.

Integration is the final stage in the process. It involves integrating the criminal proceeds into the legitimate economic and financial system, and assimilating it with other assets in the system. Integration of the 'clean' money into the economy is accomplished by the money launderer making it appear to have been legally earned or obtained.

There is potential for the money launderer to use gambling at every stage of the process. The

gambling industry is particularly vulnerable during the placement stage as the use of cash is prevalent and the provenance of such cash is not always easy to determine.

Casino and gaming house operators should be mindful that the offence of money laundering also includes simple criminal spend (the use of criminal proceeds to fund gambling as a leisure activity), and may not include all the typical stages of the laundering process (if any at all).

Money laundering in the gambling sector may take two main forms:

- Exchanging money, assets, goods and property that were acquired criminally for money or assets that appear to be legitimate or 'clean' (so called *classic money laundering*). This is frequently achieved by transferring or passing the funds through some form of legitimate business transaction or structure.
- The use of criminal proceeds to fund gambling as a leisure activity (so called *criminal or 'lifestyle' spend*).

Operators should be aware that there is no minimum financial threshold for the management and reporting of known or suspected money laundering or terrorist financing activity.

Terrorist financing is defined under section 2 of the UN Sanctions Acts which means the financing of terrorist, terrorist acts and terrorist organisations.

Financing of Terrorism is the process by which funds are provided to an individual or group to fund terrorist activities. Unlike money laundering, funds can come from both legitimate sources as well as from criminal activity for the financing of terrorism. Funds may also originate from personal donations or disguised as profits from businesses and charitable organizations and used to finance terrorism. Funds may also come from criminal sources, such as drug trafficking, smuggling of weapons (or humans) and other goods, fraud, kidnapping and extortion.

Unlike money laundering, which precedes criminal activity, with financing of terrorism, it is possible to have fundraising or a criminal activity generating funds prior to the terrorist activity actually taking place. However, similar to money launderers, those financing terrorisms also move funds to conceal their source of those funds. The motive is to validate transactions and to obscure transaction trails which could be of incriminating evidence.

2. BACKGROUND INFORMATION

2.1 The Financial Action Task Force

The Financial Action Task Force (FATF) was established in 1989 by the G7countries. It is an inter-governmental body whose purpose is to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, financing of terrorism and other related threats to the integrity of the international financial system. The FATF standards are reflected in its 40 Recommendations issued in February 2012. These are universally recognised as international standards for anti-money laundering and countering financing of terrorism (AML/CFT).

The FATF issued a first report containing a set of Forty Recommendations, for the prevention of money laundering in April 1990. These 40 Recommendations were first revised in 1996. Subsequently, in October 2001 the FATF issued the Eight Special Recommendations to deal with the issue of financing of terrorism and added a ninth Recommendation in 2004. The continued evolution of money laundering techniques led the FATF to revise the FATF standards comprehensively in June 2003. The revision brought a number of changes and one of the changes related to the classification of casinos as Designated Non-Financial Businesses and Professions' (DNFBPs) by the FATF. This change means that casinos (including gaming houses for Mauritius) are now subject to the same Anti-Money Laundering and Combating Financing of Terrorism (AML/CFT) requirements as real-estate promoters, accountants, lawyers, dealers in jewellery. The most recent revision of the FATF recommendations was effected in June 2019 and the 40+9 Recommendations were merged into 40 Recommendations. Currently the membership of the FATF includes 36 members and 8 Associate Members, including the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG).

2.2 Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)

Mauritius is a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), a regional inter-governmental body established to combat money laundering and terrorism financing in the eastern and southern African region. ESAAMLG members adopted a Memorandum of Understanding which established the Group and provided the basis

that would enable them to forge the process of cooperation for implementing the Recommendations of the Financial Action Task Force (FATF). In February 2012, the FATF issued revised Recommendations which set out a number of new requirements compelling its members to implement in order to effectively combat money laundering and terrorism financing. Mauritius was assessed by ESAAMLG in relation to its anti-money laundering and counter-terrorist financing (AML/CFT) system, using the FATF Assessment Methodology 2013. The assessment comprised a comprehensive review of the effectiveness of Mauritius' AML/CFT system and its level of compliance with the FATF Recommendations.

The Mutual Evaluation Report (MER) was published in September 2018. The MER has identified the strengths and weaknesses of the systems and procedures in place in Mauritius for combating money laundering and terrorism financing and has made a number of recommendations to enable Mauritius improve its systems and procedures. On the basis of the results of the mutual evaluation, Mauritius was placed under ESAAMLG's enhanced follow up procedures. Accordingly, Mauritius has to report bi-annually on the progress that it is making in implementing the recommended actions contained in the MER.

In this respect, Mauritius has amended the FIAMLA, POCA, POTA and enacted the FIAML Regulations and UN Sanctions Act in order to meet the FATF requirements and improve its AML/CFT framework. As it currently stands, all statutes pertaining to AML/CFT apply to all Financial Institutions (FIs) and the Designated Non-Financial Businesses and Professions (DNFBPs).

Recently, the Anti-Money Laundering and Combating of the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019 (AMLCFTAP) was enacted and came into force on 29 May 2019. The objective of the Act is to amend various enactments (including the Companies Act 2001, the Banking Act 2004, the FIAMLA and the Financial Services Act (FSA) 2007 with a view of meeting international standards of anti-money laundering and combating the financing of terrorism and proliferation and to address threats to international peace and security.

The AMLCFTAP has repealed Part 2 of the First Schedule of the FIAMLA (which previously set out a list of countries where overseas financial intelligence units are constituted) and has

replaced it with a list of transactions, which when being undertaken, members of a relevant profession or occupation must comply with the applicable provisions of FIAMLA and the rules, regulations or guidelines made or issued thereunder. An example of such a transaction is where a person licensed, under the Gambling Regulatory Authority Act, operates a casino and gaming house in which any of his customers engages in financial transactions equal to or above Mur 20,000 or an equivalent amount in foreign currency.

2.3 AML/CFT Conventions ratified by Mauritius

Mauritius has also ratified a number of AML/CFT Conventions. In March 2001, Mauritius acceded to the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, known as the Vienna Convention. On 18 April 2003, we have also ratified the United Nations Convention against Transnational Organised Crime known as the Palermo Convention. The UN Convention against Corruption was ratified on 14 December 2004. Mauritius has also ratified International Convention for the Suppression of the Financing of Terrorism on 11 December 2004.

3. THE RISK BASED APPROACH

3.1 Risk management is a dynamic tool

A money laundering/terrorist financing risk assessment is not a one-off exercise. Casino and gaming house A operators must therefore ensure that their policies, procedures and controls for managing ML/TF risks, are kept under regular review. For example, industry innovation and new products may expose operators to new emerging ML/TF threats and vulnerabilities and thus a regular assessment of risks shall be paramount before implementing new product, system, processes and business developments.

Casino and gaming house A operators need to regularly identify, re-assess and manage ML/TF risks, just like any other business risk. Operators should assess the level of risk in the context of how their business is structured and operated, and the controls in place to minimize the ML/TF risks posed. The risk-based approach evokes a focus of resources on the areas which represent the greatest risk. The benefits of this approach bring forth a more efficient and effective use of resources, the reduction of compliance costs and an efficient response mechanism to new emerging ML/TF risks.

At the core of the risk-based approach, there shall be a decision-making process on whether and/or when customer identification and verification should be conducted. Casino and gaming house A operators must determine the extent of their CDD measures, on a risk-sensitive basis depending on the risk posed by the customer and their level of activity. In order to be able to monitor customer activity, it is fundamental that monitoring commences at the early stages of the business relationship. The monitoring of customer activity should also be carried out via a risk-based approach, thus higher risk customers are expected to undergo a more frequent and rigorous scrutiny than lower risk customers. The effectiveness of this will be determined by the systems and controls mechanisms adopted by operators which will allow them to identify and monitor player activity whenever red flags and typologies are observed. This requires an effective AML/CFT design and application.

3.2 Risk Categories

The factors described below are intended to act as a guide to help casino and gaming house A operators to conduct their own customer risk assessments, and to devise AML/CFT policies and procedures which accurately and proportionately reflect those assessments. ML/TF risks may be measured using a number of factors. Application of risk categories to customers and situations can provide a strategy for managing potential risks by enabling casino and gaming house operators to subject customers to proportionate controls and monitoring. The four risk pillars within the gambling and gaming industry are;

- Country or geographic risk;
- Customer risk;
- Transaction risk; and
- Products and service risk

3.2.1 Geographical risk

Some jurisdictions pose an inherently higher ML/TF risk than others. In addition to their individual risk assessment, casino and gaming house A operators should take into account a variety of other credible sources of information in order to determine the risk of a particular jurisdiction which customers are associated with, as a result of their; citizenship; business; place of residence, and other social contexts which may require enhanced due diligence or additional verification.

Where casino and gaming house A operators need to carry out particular assessments of Geographical Risk, they may be able to do so through open source checks such as the internet or otherwise by consulting with databases dedicated on corruption risk indices which are traditionally published by specialised independent bodies. Some of these reputational bodies are Transparency International Corruption Perceptions Index, the International Monetary Fund (IMF), the Basel Institute of on Governance (Basel AML index), FATF country evaluation reports and World Bank Organisation. These sources are not exhaustive and an unending list of other sources and service endure, thus casino and gaming house A operators are urged to explore and find their right combination of tools to be used, depending on the nature of their

Geographical Risk exposure.

Ultimately, casino and gaming house A operators may decide to lower their risk appetite with other jurisdictions which are not necessarily rated as 'high-risk' with official sources. The determination of Geographical Risk should be determined through an incorporated approach between official independent guidance and the subject entities' individual assessments and experiences which could factor in, previous adverse experiences with customers from particular jurisdictions. Nevertheless, the decision to establish a business relationship or otherwise with a customer should not be solely determined by the nationality or affiliations, but through an overall risk assessment which encapsulate all risk categories in this section.

3.2.2 Customer risk

Determining the potential ML/TF risks posed by a customer, or category of customers, is critical to the development and implementation of an overall ML/TF risk-based framework. Based on their own criteria, casino and gaming house A operators should seek to determine whether a particular customer poses a higher risk in terms of ML/TF. This section brings to context scenarios where customers may be deemed as higher risk however these are merely guidelines and should be solely used as foundations for the casino and gaming house A operators individual risk assessment and compounded with all the other relevant risk categories referred to in this section.

- **High Rollers;**

The determination of a high roller will vary from one operator to another. Casual customers which deposit high stakes in a limited time-span, perhaps even during a single visit, may be considered as a high roller. These are also commonly referred to as VIP customers. Most casino and gaming house A operators will have policies designed for these type of customers and such policies may relate to commercial risk, or to marketing strategies which identify and attract high spending customers into casinos and gaming houses which are typically provisioned with complementary goods and services such as refreshments, food, entertainment, merchandise, lodging, show tickets and tickets to special events and transportation. Occasionally, casinos and gaming houses also offer special facilities to VIP customers such as the use of VIP rooms.

Such strategies may be acceptable as long as casino and gaming house A operators ensure that AML/CFT policies, procedures and internal controls are being consistently applied as delineated in this guidance. Being a high roller, itself should not determine the customer as being high risk, however such players are the most likely to reach and exceed the pre-set thresholds thus inevitably would need to undergo the relevant due diligence and the understanding of their relevant source of wealth and funds.

- **Affordability;**

Where necessary, casino and gaming house A operators should obtain information about the customers' financial sources, otherwise referred to as Source of Wealth or Source of Funds (SOW/SOF), so that they can determine whether customers' spending is in proportion to their respective income and/or wealth. This approach will allow casino and gaming house A operators to identify changing or unusual spending patterns which are not aligned with the customer's affordability.

- **Player Collusion;**

Casino and gaming house A operators should monitor frequent even money wagering, particularly when conducted by a pair of better covering both sides of an even bet (e.g. roulette, baccarat, or craps) or otherwise two or more customers frequently wagering against one another on even-money games. Another typology which is commonly observed in the gambling sector is referred to as 'Chip dumping' which is commonly associated with poker games and is the deliberate loss of money or chips to another player allowing for the disguise of illegitimate funds to legitimate during the process. Another form of collusion could manifest between the player and the casino or gaming house employees thus customers trying to befriend or have a close relationship with employees should be monitored, depending as the case may be.

Where a customer is assessed as presenting higher risk, additional identification information should be conducted, always in proportion to the risk being engendered. Such information may manifest in the request of the national identity card or driving license; a valid passport; proof of a residential address, proof of occupation and where necessary their source of funds and wealth as the case may be and in respect to the transaction being made. This will help the casino

and gaming house A operators to understand further their customer profiles whilst also lowering the inherent risk through a solid mitigating mechanism. Player information should be kept on record for a minimum of seven (7) years for future reference and evidence. Whilst the GRA recognizes that some transactions with customers will be occasional by nature, particularly in the case of tourist, casino and gaming house A operators are still obliged to collect and verify the relevant information from customers, particularly when these pose a higher risk to the business.

3.2.3 Transaction risks

Some products, services and transactions are inherently riskier than others and are therefore more attractive to criminals. These include gaming products or services that allow the customer to influence the outcome of a game, be it on their own or in collusion with others. The use of specific funding methods should also be treated as inherently higher risk.

- **Use of Cash;**

The use of cash is heightened in casinos and gaming houses which constitutes a natural ML/TF threat. Through the use of cash, casinos and gaming houses are exposed to the incursion of illicit proceeds. Money launderers may attempt to refine small denominations to larger ones through the entities' financial system, which are typically easier to hide and transport. Redemption of chips, tickets or tokens for cash or cheque, particularly after minimal or no play are other transaction risks operators need to be aware of and consider with their individual risk assessment. One way of mitigating such risk is to pay out customer winnings through the same means by which the customer paid the deposit.

- **Use of third-party agents;**

Money launderers and criminals may use third parties or agents to circumvent CDD mechanisms. This requires casino and gaming house A operators to conduct the necessary due diligence and to identify the ultimate beneficiaries, particularly when dealing with agents or third

parties dealing on behalf of other person(s) such as casino junkets[1]. In addition, some customers may be used as 'mules' by criminals through 'loan sharking' or simply as vehicles which allows for the opportunity to indirectly introduce criminal proceeds into the casino and gaming House legitimate financial systems.

- **Currency Exchange;**

Players purchasing and cashing out large volumes of casino chips with little or no gaming activity should be closely monitored by casino and gaming house A operators given that this typology exposes them to the risk of layering and refining. Refining is the changing of an amount of money from smaller denomination bills into larger ones. Another refining method is the use note acceptors' or slot machines which allow for the use of cash. In order to mitigate this risk, casino and gaming house A operators should have threshold mechanisms which trigger upon a certain amount of deposits which would consequently require the customer to undergo due diligence and verification procedures.

Casino and gaming house A operators are not required to perform identification of customers for the redemption of chips, tickets, or tokens unless the customers, may on a given date, enter a cumulative financial transaction equal or above MUR 20,000. Notwithstanding, casino and gaming house A operators are expected to have the necessary mechanisms to be informed when such thresholds are met thus a standard identification process is favored upon the initiation of a business relationship.

[1] The term Junket has its origins in Chinese where Jin literally means introducing and Ke means customers. It is a method of casino marketing developed in the late 1930s for introducing customers to the expanding Macao, China gaming industry. Over time this method has been adopted elsewhere and the term has gradually evolved to be known as Junkets.

3.2.4 Product and Service risk

Casino and gaming house A operators should consider their products and services materialized in the forms of games which can be used to facilitate ML/TF. Product risk includes the consideration of vulnerabilities associated with same and the mitigating risks adopted. In casinos and gaming houses there are a number of gambling opportunities that offer the potential for a money launderer to place funds and generate a winning cheque or similar with minimal play. Also, a number of gambling activities take place in casinos and gaming houses where customers effectively play against each other. This offers the money launderer a means to transfer value by deliberately losing to the individual to whom they want to transfer the funds.

Products which may pose a money laundering risk for the casino and gaming house A operators therefore include:

- Peer to peer gaming such as Poker where player collusion could manifest;
- Gaming where two or more persons place opposite, equivalent stakes on even, or close to even, stakes (for example, the same stake on red and on black in a game of roulette, including electronic roulette) and
- Gaming machines, which can be used to launder stained or fraudulent bank notes or for the refining of smaller denomination in to larger ones.

The instances described above are not intended to be prescriptive or comprehensive. These will not apply universally to all casinos and gaming houses and even when similar risks are present, they would need to be mitigated in accordance of the nature of the business which tend to differ from one entity to another, depending upon a host of other variables which are not necessarily covered in this guidance. Notwithstanding, these variables shall be used as instances to guide further casinos and gaming houses on how to conduct their own risk assessments, and how to devise AML/CTF policies, procedures and controls which accurately and proportionately reflect those identified risks. Consequently, this guidance accentuates that the weighting given to the risk factors identified by casino and gaming house A operators when assessing their overall risk of ML/TF, shall be based on their own judgment and expertise given that each separate entity has its own different exposures and control mechanisms.

Risk levels may be impacted by a number of variables, which will also have an impact on the mitigating measures required to tackle such exposures in a proportionate manner. Risk levels may be determined by considering the following conditions;

a) Ratio of number of customers against the volumes of gaming revenues;

b) The speed and volume of business;

c) The size and dynamics of the premises;

d) The customer profile, for example whether:

   - the majority of customers are regular visitors or are members;
   - the casino and gaming house rely on tourists and
   - the casino and gaming house rely on junkets.

e) Whether the casino and gaming house has VIP rooms or other facilities for High rollers;

f) The types of financial services offered within the casino and gaming house such as currency exchange;

g) The types of payment methods accepted;

h) Staffing levels, experience and turnover;

i) The existing mitigating controls and supervision measures adopted by the casino and gaming house;

j) Whether the casino and gaming house falls under a Corporate entity and is part of a chain of other leisure facility.

International Case Study of Money Laundering

- A drug dealer, whose only legitimate source of income for ten years was state benefits, spent more than £1million in various gambling establishments over the course of two years, and lost some £200,000. All the transactions appeared to involve cash.
- A customer spent a large volume of cash at a casino, including a significant quantity of Northern Irish and Scottish bank notes. The customer told staff that the cash came from restaurants and takeaway food establishments that they ran around the United Kingdom. This explanation was accepted at face value by the staff, however, in reality the customer did not own any legitimate businesses and was later convicted of money laundering offences arising from criminal activity.

Whilst this guidance acknowledges ML/TF risks will never be totally eliminated, returning winning funds in the same form the deposits were made, (for example in cash), limits the opportunity for money launderers to layer their illicit proceeds. Where it is not feasible to return funds to the source in the same form, casino and gaming house A operators should have right controls in place in order to mitigate the risk of ML/TF.

4. GOVERNANCE FRAMEWORK

The Board of Directors are ultimately responsible for the overall business strategy of Casinos and Gaming Houses A and thus, are in the best position to advocate an AML/CFT compliance culture and to determine the right approach toward the potential risks that casino and gaming house may be exposed to.

As part of its compliance obligations, and pursuant to Section 113C of the GRA Act, casino and gaming house A operators are obliged to appoint and register a Money Laundering Reporting Officer (MLRO) with the GRA, who shall assist the Board with the implementation and overlooking of a robust AML/CFT framework and to ensure that the relevant policies and procedures are being adhered to, in accordance with the obligations under the FIAMLA and FIAML Regulations 2018.

With the aid of the MLRO, the Board of Directors should endorse an action plan for the conducting of an overall AML/CFT Business Risk Assessment (hereinafter referred to as BRA), which should delineate all four risk pillars as explained in section 3.2, and ensure that this remains relevant with the latest ML/TF trends and typologies that the business may be exposed to. Similarly, it is recommended that a risk appetite which shall determine the Customer Acceptance Policy of casinos and gaming houses is determined and endorsed by the same board.

On the basis of its BRA, a subject entity must establish a strategy to counter ML/TF within its operations. A good governance mindset requires that this strategy is clearly documented and communicated with the rest of the organisation through the relevant policies, training and procedures of the applicable systems and controls adopted. The Board of Directors should also endorse a clear escalation procedure for the reporting of suspicious activity, by mainly defining the roles and responsibilities of the Money Laundering Reporting Officer (MLRO), the Deputy MLRO (whenever required), and the Compliance Officers which are responsible for the day to day aspect of operations. A risk-based approach mentality is recommended when devising an AML/CFT strategy which should allow for a better use of resources by emphasizing the relevant controls and mechanisms on higher ML/TF risks and vulnerabilities.

Ultimately, the Board of Directors should revaluate and reconsider the appropriateness and

effectiveness of its AML/CFT framework and its policies and procedures through the expertise of the MLRO, at least on an annual basis, or whenever material changes to the casino and gaming house occur such as the introduction of new products and services, change of systems and procedures or natural new emerging ML/TF threats and vulnerabilities. Where, as a result of its review, changes or review of policies and procedures are required, the Board of Directors and the MLRO, must ensure that the casino and gaming house makes the necessary changes, in reasonably timely manner.

4.1 The Money Laundering Reporting Officer (MLRO)

In accordance with Regulations 26(1) of FIAML 2018, and Section 113C of the GRA Act, casino and gaming house A operators shall appoint and register a Money Laundering Reporting Officer (MLRO), who shall be responsible for the overlooking of the subject entities' AML/CFT framework and to ensure that adherence to the relevant AML/CFT policies and procedures are made across the organisation. The role of the MLRO is onerous and not to be undervalued, thus an adequate number of hours should be allowed to conduct this duty, depending as the case may be.

Regulation 26(4) of the FIAML Regulations 2018, affirms that MLRO's should be of a sufficient senior role in the organisation and should have enough experience, authority, and the right of direct access to the board of directors. The MLRO should also have adequate time and resources to effectively perform his or her functions. A good governance culture requires that a clear and robust escalation procedure and controls are in place which allow Compliance officers and other designated personnel, to escalate internal suspicious reports with the MLRO, whenever risk indicators are observed during the course of a business relationship. It is ultimately the responsibility of the MLRO to determine if an STR should be disclosed with the FIU or otherwise.

Copies of STR forms disclosed with the FIU, together with any relevant documentation submitted as part of, or together with the STR itself, should be retained by the subject person for any such period as may be specified in the written notice given by the Director of the FIU. This period starts to run on the date when the report was submitted to the FIU. Furthermore, an internal suspicious report escalated with the MLRO, which has not given rise to a disclosure

with the FIU, should also be maintained by the subject entity for a period of seven (7) years along with a documented rationale as to why the disclosure was not made. The seven year period in this case, commences to run on the same date when the MLRO reaches the determination not to escalate the report with the FIU. The MLRO should be readily available as shall be the main point of contact with the FIU when handling suspicious disclosures, thus also requires that the MLRO has unrestricted access to the relevant CDD information and systems of the casino's and gaming house's customers;

In its supervisory functions, the GRA may require casino and gaming house A operators to demonstrate the MLRO's quota of time allocated to perform his or her role and the available resources the MLRO enjoys. In addition, GRA may also request copies of internal suspicious reports which have not given rise to a disclosure for a better evaluation and determination of the casino and gaming house controls. Failure to effectively and satisfactorily demonstrate the above may result into a potential breach of Regulation 26(4) (b) of FIAML Regulations 2018.

4.2 Deputy Money Laundering Reporting Officer (DMLRO)

A casino and gaming house A operator may decide to appoint a Deputy Money Laundering Reporting Officer ("DMLRO") in order to exercise MLRO functions in his or her absence. Given the functions that the MLRO has to carry out, it is imperative that he or she is available at all times, however, it is recognised that this is not always possible and that, depending on the business, the volume of internal and external queries may undermine the MLRO's effectiveness. To this end, the designated officer (deputy MLRO), may temporarily replace the MLRO when absent whilst also determining in his/her own right that an STR is to be filed in those situations when the MLRO is absent. The DMLRO should enjoy *akin* status and experience of the MLRO.

Where the same person acts as MLRO on multiple casinos and gaming houses, he or she should ensure that the employment conditions are in accordance with FIAML Regulations 2018.

4.3 Compliance Officer(s)

In accordance with Regulations 22 (1) (a) of FIAML Regulations 2018 and the guidelines, the

casino and gaming house A operator shall designate a Compliance Officer at senior management level. The Compliance Officer is responsible for the implementation and ongoing compliance of the casino and gaming house with internal programmes, controls and procedures with the requirements of the FIAMLA and FIAML Regulations 2018. Senior management is defined under the FIAML Regulations 2018 as an officer or employee with sufficient knowledge of the institution's ML/TF risk exposure and sufficient seniority to take decisions affecting its risk exposure, and have direct access to board of directors.

The Compliance Officer appointed by the casino and gaming house A operator must:

a) be a natural person;
b) be of at least senior management level as defined under FIAML Regulations 2018; and
c) have the appropriate qualification knowledge, skill and experience to fulfil a compliance role within the casino and gaming house;

The casino and gaming house operator must ensure that the Compliance Officer:

a) has timely and unrestricted access to the records of the casino and gaming house;
b) has sufficient resources to perform his or her duties;
c) has the full co-operation of the casino and gaming house staff;
d) is fully aware of his or her obligations and those of the casino and gaming house; and
e) reports directly to, and has regular contact with, the Board so as to enable the Board to satisfy itself that all statutory obligations and provisions in FIAMLA and FIAML Regulations 2018, and the guideline are being met and that the casino and gaming house is taking sufficiently robust measures to protect itself against the potential risk of being used for ML and TF.

In accordance with Regulations 22(3) of the FIAML Regulations 2018, the functions of the Compliance Officer include:

a) ensuring continued compliance with the requirements of the FIAMLA and FIAML Regulations 2018 subject to the ongoing oversight of the Board and senior management of the casino and gaming house;

b) undertaking day-to-day oversight of the program for combatting money laundering and terrorism financing;

c) regular reporting, including reporting of non-compliance, to the Board and senior management; and

d) contributing to designing, implementing and maintaining internal compliance manuals, policies, procedures and systems for combatting money laundering and terrorism financing.

While it is not anticipated that the Compliance Officer will personally conduct all monitoring and testing, the expectation is that the Compliance Officer will have oversight of any monitoring and testing being conducted by the casino and gaming house.

The circumstances of the casino and gaming house may be such that, due to the small number of employees, the Compliance Officer holds additional functions or is responsible for other aspects of the casino's and gaming house's operations. Where this is the case, the casino and gaming house must ensure that any conflicts of interest between the responsibilities of the Compliance Officer role and those of any other functions are identified, documented and appropriately managed. The Compliance Officer however should be independent of the core operating activities of the casino and gaming house.

For the avoidance of doubt, the same individual can be appointed to the positions of Money Laundering Reporting Officer ("MLRO") and Compliance Officer, provided the casino and gaming house considers this appropriate with regard to the respective demands of the two roles and whether the individual has sufficient time and resources to fulfil both roles effectively.

4.4 Screening of Employees and Third Parties

Another good governance standard is to carry out onboarding and ongoing screening checks of the relevant casino and gaming houses employees. Besides an in-depth assessment of the skills,

knowledge and expertise of their applicants, casino and gaming house A operators are recommended to carry out a personal conduct due diligence check, with the for instance requesting the certificate of character issued from the by the Office of the Director of Public Prosecutions (DPP) particularly with prospect employees which shall be designated with Compliance duties or otherwise are more exposed to collusion and exploitation. Similarly, casino and gaming house A operators are expected to conduct the relevant screening and due diligence with its third parties and business relationships. The relevant third-party agreements may also be requested by the GRA in order to conduct its supervisory functions on AML/CFT thus it is expected that these are also made readily available upon request, as the case may be.

4.5 Audit Function

Casino and gaming house A operators should conduct an independent audit on a periodical basis of at least once a year, which could be managed by either the entities' internal audit function (if applicable) or otherwise through an outsourced third-party service which specializes on AML/CFT compliance audits. The main motive and objective of such audit is to assess and evaluate the adequacy and effectiveness of the relevant AML/CFT policies, procedures, and controls implemented by the operator. In addition, following the conducting of an audit, a detailed findings report should be documented and recorded by the operator. Any recommendations made by the relevant auditors should be followed up and conformed in a reasonably timely manner. Through its supervisory powers, the GRA may request evidence of all AML/CFT audits conducted by operators thus it is expected that these are archived and made readily available for AML/CFT supervisory purposes.

4.6 Training

Paragraph 22 (1) (c) of the Financial Intelligence and Anti-Money Laundering Regulations 2018 requires that casino and gaming house A operators to conduct an ongoing training program for its Board of directors, senior management and other employees pertinent to the AML/CFT framework in order to maintain awareness of the relevant AML/CFT Laws and Regulations and the latest threats and vulnerabilities induced by ML/TF. Casino and gaming house A operators should also ensure that regular training and briefings are made with their resources on their policies, procedures and controls. A general understanding of the FIAMLA

Regulations 2018, the FIAMLA 2002, The Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019, the Gambling Regulatory Authority Act 2007 and the United Nations Sanctions Act 2019, is important and compliance personnel must be conversant with the same, particularly the MLRO and the DMLRO (when applicable).

One of the key control mechanisms for the prevention and detection of money laundering is to have dedicated employees who are monitoring and addressing risks of ML/TF, which are well trained in the identification of unusual activities or transactions which appear to be of a suspicious nature, as well as having the ability to perform an accurate verification of customers' identity when necessary. Reporting and escalation of matters that give grounds for suspicion of ML/TF is an important key element which should be covered in the training of such employees. The effective application of a solid AML/CFT control mechanism can be quickly undermined if the employees administering the system are not adequately trained. The continuity of resource training is thus of an utmost importance for a successful AML/CFT strategy. Additionally, casino and gaming house A operators are also expected to monitor the effectiveness of such training and to ensure that gaps are addressed in an appropriate and timely manner whilst reinforcing the assertion that the training being provided is indeed satisfactory.

Under FIAMLA 2002 and the Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019, individual employees may face criminal prosecutions should these be found guilty of deliberately facilitating ML/TF. It is therefore important that employees are made aware of such legal liabilities, and are given adequate training on how to conduct AML/CFT functions.

In summary, casino and gaming house A operators should ensure that their relevant employees are conversant with;

- their responsibilities under the operator's policies and procedures for the prevention of ML/TF;
- the identified ML/TF risks from the operator's business risk assessment;

- the operator's procedures and control mechanisms for managing the same risks identified;
- the identity, role and responsibilities of the nominated officer(s) (MLRO and/or Deputy MLRO) and how to interact with either, according to the operator's policies and procedures;
- the potential effects of an AML/CFT breach on the operator and its employees;
- the operators' Customer Due Diligence and Enhanced Due Diligence procedures;
- how the operator will monitor customers when CDD is not undertaken upon entry at the casino;
- how PEP's, their family members and their known close associates shall be identified and verified, and
- how to acquire senior management approval to conduct a business relationship with a PEP.

Policy and procedure manuals, whether physical or electronic, are useful in raising employee awareness on ML/TF and can serve as a good baseline for a solid understanding of what is expected from them, nevertheless, policies and procedures should not replace the concept of dedicated training sessions, thus it is expected that ongoing training is provided to all relevant employees at appropriate intervals such as when new products or business developments are introduced or when AML/CFT legal amendments have been enacted. Furthermore, training records should be maintained in order to have a register of trained employees, dates when the training was conducted, the nature and format of the training and the overall assessment of the training provided through employee feedback forms (when applicable). There is no one-size-fits-all solution when determining how to deliver training and a lot of this shall be determined by the size and nature of the business however, it shall be the liability of an experienced MLRO to determine the skill gaps and training requirements that front-line resources require.

Additional instruments and literature pertinent to AML/CFT may be accessed on GRA's website such as the National Risk Assessment, FATF Risk Based Approach and other relevant guidance pertinent to AML/CFT methodologies, which casino and gaming house should make

use of, particularly with their employees and where necessary by incorporating these with training programs.

4.7 Policies, Procedures, and Controls

Casino and gaming house A operators must establish and maintain policies, procedures and controls to mitigate and manage effectively the risks identified in the operator's AML/CFT risk assessment. The same policies, procedures and controls must be proportionate to the size and nature of the operator's business and dated, approved, and signed by the relevant casino and gaming house senior management.

Pursuant to section 19J (1) of the FIAMLA 2002, the GRA may, in the discharge of its supervisory functions, require casino and gaming house operators to make available any information and produce any record or document within such time and at such place as it may determine.

Casino and gaming house A operators are expected to maintain detailed documentation pertinent their own policies, procedures and controls and an updated log amendment performed, as the case may be. In addition, it is recommended that the communication methods used with the rest of the organization in relation to the same policies and procedures, are also kept on record for potential supervision matters.

Notwithstanding the above, the policies, procedures and controls should include:

- Risk management practices;
- Internal control mechanisms;
- CDD and ongoing monitoring measures, including enhanced measures for higher risk PEP profiles customers;
- Record keeping procedures;

- The monitoring and management of compliance and the internal communication strategies used to communicate policies, procedures, and controls; and
- Procedures pertinent to the escalation of Suspicious Transaction Reports.

The policies, procedures and controls must include specifics which:

- provide for the identification and scrutiny of:
    - complex or unusually large transactions, or unusual patterns of transactions, that have no apparent economic or legal purpose
    - and other activity or situation that the casino and gaming house operators regards as particularly likely, by its nature, to be related to money laundering or terrorist financing
- specify the undertaking of additional measures, where appropriate, to prevent the use for money laundering or terrorist financing of products or transactions that might favour anonymity;
- enable personnel who knows or suspects, or has reasonable grounds for knowing or suspecting, money laundering or terrorist financing to report such knowledge or suspicion to the Money Laundering Reporting Officer particularly by;
    - defining the procedures for handling STR's, covering both the full process flow from the reporting of employee to the submission to the FIU;
    - defining the communication mechanisms between the nominated officer and law enforcement and/or the FIU;
    - defining recording methods of information not acted upon by the MLRO, with an appropriately documented rationale as to why no further action was taken;
    - defining the reporting communication lines between the nominated officer (Compliance Officer, MLRO and Deputy MLRO) and senior management;
- specify which systems are adopted for customer identification and verification, including enhanced arrangements for high risk customers, including PEPs;

- define the circumstances where additional information in respect of customers will be sought in the light of their activity and risk assessment;
- specify how the business will ensure compliance with internal policies, procedures, controls and on-going monitoring;
- define the communication methods of such policies, procedures and controls, including details of how compliance is monitored by the nominated officer, and the arrangements for communicating the same with all relevant employees;
- methods how casino and gaming house operators will communicate and make sure that policies, procedures and controls are established and harmonised across their branches/outlets (when applicable).

5. CUSTOMER DUE DILIGENCE (CDD)

5.1 Introduction

As per FIAML Regulations 2018 and GRA Act 2007, casino and gaming house A operators are obliged to conduct the necessary identification, verification and customer due diligence (CDD) upon a set of particular thresholds. Such measures apply when:

- operators engage in a financial transaction[2] with a customer equal to or above 20,000 rupees or an equivalent amount in foreign currency;
- a person withdrawing a winning equal to or above 20,000 rupees;
- the operator becomes aware that the circumstances of an existing customer risk profile has changed during the course of a business relationship; or
- an occasional transaction[3] equal to or above 20,000 rupees

Notwithstanding the above, casino and gaming house operators are obliged to report when they suspect that customers are performing suspicious activity even when the financial amounts do not meet or exceed the set thresholds referred to hereinabove.

5.2 Thresholds

Casino and gaming house operators tend to induce a fast movement environment of financial transactions and people by nature, thus an 'on-entry' identification measure prior the entry of

[2] For the purpose of this guidance, a 'Financial Transaction' consists of the wagering of stakes, including: the purchase from, or exchange with, the casino of tokens for use in gambling at the casino or a direct payment both in cash or digital, for the use of gaming machines. For the avoidance of doubt, a 'Financial Transaction' shall exclude any bonuses, winnings or other financial benefits which are granted by the Casino or Gaming Houses during the course of a business relationship or an occasional transaction.

[3] "occasional transaction" means any transaction carried out other than in the course of a business relationship;

a gaming premises is recommended. Additional information such as the verification of identity and information pertinent to the source of wealth and source of funds of the customer, may be deferred until the pre-set thresholds are met and in accordance to the risk engendered with the main motive to reduce the disruption of the business as much as possible. Notwithstanding, verification measures and a customer specific risk assessment which determines the type of due diligence to be conducted should be in place when customers reach or exceed the indicated thresholds hereinbelow. Paragraph (a) Part II of the Transactions Undertaken By Members of a Relevant Profession or Occupation of the Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation (Miscellaneous Provisions) Act 2019, specifies that a person licensed under the Gambling Regulatory Authority Act to operate a casino and gaming house amongst other, should conduct the necessary due diligence measures where a financial transactions are equal to or above 20,000 rupees or whenever an equivalent amount in foreign currency is met. Moreover, section 105 (1) (a) (aa) of the Gambling Regulatory Authority (GRA) Act 2007 obliges operators to record the name, surname and NIC number of a person receiving a winning which meets or exceeds the amount of 20,000 rupees.

A threshold applies when the wagering of stakes is either in a 'single transactions' or transactions which appear to be linked through a series of activity which, when taken cumulatively, reach or exceed the total of 20,000 rupees on any given date[4]. Transactions may be also considered to be linked if carried out by the same customer through the same game or in a single gaming session. Such scenarios are not exhaustive and casino and gaming house operators should consider whether there are other circumstances where transactions may be linked. Ultimately, casino and gaming house operators should ensure that the relevant control measures are in place to prevent customers from systematically spreading their wagering or collection of winnings in a way to circumvent the applicable thresholds and CDD requirements. When casino and gaming house operators are unable to complete the CDD of a customer, they should

[4] "given date" means a period of 24 hours starting at 10 o'clock in the morning on a day and ending at 10 o'clock in the morning on the following day;

terminate their business relationship or otherwise refrain from entering a new one.

Casino and gaming house operators are commended to implement the relevant mechanisms and timing for their verification procedures and to conduct necessary enhanced customer due diligence whenever high-risk situations manifest, particularly upon customers reaching the thresholds. Akin to this, existing customers which fall outside of their risk profile during the duration of a business relationship, should also undergo additional due diligence measures. In determining when it is appropriate to apply CDD measures with existing customers, casino and gaming house operators should consider:

- any indication that the details of an existing customer have changed;
- any transactions which is not reasonably consistent with the customer's affordability; and
- any other matter which may influence the operator's customer risk assessment in relation to ML/TF.

Gaming Machines:

The threshold limit applies even when 'cash accepting' Gaming Machines such as Slots Machines products are being offered, however not in isolation from the rest of the offered products. These types of products induce another opportunity for customers to circumvent the relevant set thresholds. In view of this, it is paramount to factor in, cash accepting products, with the rest of the cumulative spending of the customer. Consequently, casino and gaming house operators should avoid making separate distinctions from the exchange of tokens and other games which accept direct cash from the customer, such as gaming machines.

For the avoidance of doubt, casino and gaming house operators need to set the right control mechanisms in order to monitor the full trail of customer spending during the duration of a business relationship which may include both the exchange of casino and gaming house tokens for direct cash and the direct acceptance of cash through products such as Gaming Machines.

5.3 Customer Due Diligence (CDD) Measures

For the purpose of this guidance, Customer Due Diligence measures shall entail the identification of a customer using reliable source such as; an official Identity Card, a valid Passport or a valid Driving License, unless otherwise the identity of a customer is known to the casino and gaming house operators through previous interactions and identification procedures. The secondary aspect of Customer Due Diligence is the verification of the customer's identity. In the context of casinos and gaming houses, the verification process may be completed during the identification stages since official document pertinent to the customer is requested upon entry, particularly in brick and mortar establishments.

5.3.1 Identification

For the avoidance of doubt, casino and gaming house operators should identify their customers by requesting:

a) name and surname;
b) residential address; and
c) date of birth

In the case of casino and gaming house operators, this information may be gathered using identification documents, such as national ID cards, passports, or official documentation from governmental bodies such as birth certificates. Other documentation may be considered valid however this shall always be at the discretion of Casinos and Gaming Houses.

5.3.2 Verification

The requirement for verification procedures are compulsory when customers reach or exceed the indicated thresholds discussed in section 5.2. For the avoidance of doubt, casino and gaming house operators should verify their customers by requesting and verifying the following details:

d) identity reference number;

e) nationality;

f) place of birth; and where necessary

g) employment information.

For the purposes of this guidance, 'verify' means the verification of a customer's identity through the collection of documents or information which must be obtained from reliable and independent sources. Documents issued by an official governmental body should be regarded as being independent and reliable.

Dependent on the customer risk profile, casino and gaming house operators should request and verify the source of funds and source of wealth of customers in order to justify the gaming activity. This shall be particularly important whenever customers are deemed to be of a higher risk profile, as previously delineated in this guidance.

By obtaining and physically reviewing original documents, casino and gaming house operators would be ensuring that the relevant verification obligations are being adhered to. The measure is augmented when the relevant checks are being made in relation to the same person the operators are conducting a business relationship with such as comparing the photographic evidence of documents with the customer facial features and ensuring that the same documents are valid and genuine.

5.3.3 Third Party Agents

In such cases where agents or when a beneficial owner is represented by another third party, casino and gaming house operators are obliged to conduct the relevant due diligence measures in order to identify and verify the identity of a beneficial owner whom shall enjoy the winnings. For the avoidance of doubt, when a third party is allowed to act on behalf of another customer (such as in the case of Casino Junkets), casino and gaming house operators should:

- verify that the person is authorised to act on the customer's behalf for instance through signed declaration form and other means which are sufficiently acceptable for casinos and gaming houses; and

- identify and where necessary verify the person's identity on the basis of documents or additional information which are obtained from reliable and independent sources.

In terms of Customer Due Diligence, casino and gaming house operators shall meet the requirements set out in this guidance through an overarching evaluation of risks which shall be induced by the same AML/CFT risk assessment and their final Customer Acceptance Policy which will differ from one business to another depending on the gross exposures of ML/TF risks and the relevant control mechanisms implemented. Operators are thus urged to move away from any prescriptive methods and to instead adopt a 'risk-based approach' towards the mitigation of risks through CDD. For the avoidance of doubt, when assessing their gross level of risk exposures and the depth of CDD to be conducted, casinos and gaming houses operators should consider:

- the purpose of a customer transaction;
- the size of the transactions undertaken by the customer;
- the duration of the business relationship; and
- the risk profile of the customer.

5.4 Enhanced Due Diligence (EDD)

For an Enhanced Due Diligence process, operators may consider adequate third-party services which specialise on CDD and have direct access to multiple sources which allow for an in-depth understanding of a natural person or legal entity. Notwithstanding, operators should ensure that they are not dependent on one source of information and to adopt a diversified approach in order to ensure that an accurate description of the customer profile is made. For the avoidance of doubt, casino and gaming house A operators should apply Enhanced Customer Due Diligence by conducting:

- an in-depth background check of a natural person or legal entity with the motive to gain an understanding pertinent to adverse media articles and the potential risk of involvement in schemes pertinent to AML/CFT;

- enhanced ongoing monitoring of transactions, with the motive to determine whether these appear to be of a suspicious nature;
- enhanced ongoing monitoring of transactions, with the motive to determine that the transactions are consistent with the customer's affordability; and
- additional measures to understand, where necessary, the sources of wealth and sources of funds used by a natural person or a legal entity to make a transaction;

For the avoidance of doubt, casino and gaming house operators must apply enhanced customer due diligence (EDD) measures and enhanced ongoing monitoring over and above the required CDD measures in order to mitigate the ML/TF risks engendered in the following cases:

- where the operator is incredulous of the customer's information or otherwise has reasonable grounds to suspect that that a customer has provided false information or a stolen identity of another individual.
- where a transaction is complex or unusually large, or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic or legal purpose;
- whenever casino and gaming house operators enter into a business relationship with a PEP;
- whenever there is suspicion that the customer is subject to sanctions or freezing of assets as identified by the United Nation Consolidated List;
- when a natural person or a legal person has direct affiliations, being of a business or a personal nature, to a high-risk jurisdiction; or
    - as identified as having significant levels of corruption; or
    - a sanctioned or embargoed jurisdiction issued by the European Union or the United Nations; or
    - a jurisdiction identified to have direct links and / or supports terrorism groups by internationally independent bodies.
- when the product or transaction favours anonymity;

- when payments are received from an unknown or an unrelated third party of the customer;
- when the transaction involves a significant amount of cash;
- whenever a transaction is conducted in unusual circumstances;
- in any other case where the activity occurring, is considered to be of a higher ML/TF risk by the casino and gaming house operator;

5.5 Politically Exposed Persons (PEPs)

The definition of a Politically Exposed Person (PEP), as per the Financial Intelligence and Anti-Money Laundering Regulations 2018, shall be mean:

a) **Domestic PEP** means a natural person who is or has been entrusted domestically with prominent public functions in Mauritius and includes the Head of State and of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;

b) **Foreign PEP** means a natural person who is or has been entrusted with prominent public functions by a foreign country, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;

c) **International Organisation PEP** means a person who is or has been entrusted with a prominent function by an international organisation and includes members of senior management or individuals who have been entrusted with equivalent functions, including directors, deputy directors and members of the board or equivalent functions and such other person or category of persons as may be specified by a supervisory authority or regulatory body after consultation with the National Committee;

d) **Family Members** means individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership

e) **Close Associates** means individuals who are intricately connected to a PEP, either socially or professionally.

The potential risks associated with PEPs justify the application of additional anti-money laundering / counter terrorist financing (AML/CFT) preventive measures with respect to business relationships with PEPs. Considering this, the FIAML Regulation 2018 requires that casino and gaming house operators conduct enhanced due diligence measures when entering a business relationship with a foreign PEP which entails the additional verification and understanding of their Source of Wealth and Source of Funds SOF/SOW, as the case may be.

In view of this, casino and gaming house operators are urged to conduct the relevant screening checks on their existing customer base in order to determine if PEP profiles are current and to conduct the relevant enhanced due diligence measure when such profiles are identified. The use of third-party services which offer PEP databases may be appropriate for such screening, particularly when a high population of PEPs may be existent. Additionally, casino and gaming house operators may have the advantage to make use of their surveillance units in order to identify circumstances where PEPs have accessed their services.

When a casino and gaming house operator has determined that a relationship with a PEP shall be established, the operator must assess the extent of enhanced due diligence measures applied. Always depending on the operators customer risk profile, risk tolerance of operators and the relevant control mechanism in place. For the avoidance of doubt, casino and gaming house operators are required, on a risk-sensitive basis, to:

- have in place an appropriate risk management systems and procedures to determine whether a customer (or the beneficial owner of a customer) is a PEP, or a family member or known close associate of a PEP;
- have the relevant approval mechanisms in place from senior management for the establishing or continuing a business relationship with PEPs;

- take adequate measures to establish the SOW/SOF which involved in the proposed ‘business relationship’ or ‘occasional transaction’ with PEPs; and
- where a business relationship is entered, conduct enhanced ongoing monitoring of the business relationship

New or existing business relationships may not initially meet the criteria of a PEP; however, this may change over time. Akin to this, customers initially identified as PEPs may cease to be so thus a re-adjustment of the relevant on-going monitoring may be justified with such profiles. PEP statuses cease to exist, 12 months following the cessation of public positions. This requires that casino and gaming house operators should, as far as practically possible, be able to determine any changes of such status through the same screening techniques suggested above. When PEP statuses cease to exist, casino and gaming house operators are no longer required to apply enhanced customer due diligence measures with the PEP, Family Members of PEPs and Close Associates of PEPs.

6. SUSPICIOUS TRANSACTION REPORTING (STR)

As per section 14 of the FIAMLA, it is an obligation of casino and gaming house A operators to report a suspicious ML/TF transaction to the FIU, not later than 5 working days after the suspicion arose. Subject entities are required to use the standard STR form which can be found on http://www.fiumauritius.org/English/Reporting/Documents/STR_FORM_FINAL_VERSION.pdf, which the officially approved FIU form in accordance with section 15 of the FIAMLA.

A 'Suspicious transaction' is defined under FIAMLA as a transaction which:

(a) gives rise to a reasonable suspicion that it may involve:

(i) the laundering of money or the proceeds of any crime; or

(ii) funds linked or related to, or to be used for, financing of terrorism or by proscribed organizations, whether or not the funds represent the proceeds of a crime;

(b) is made in circumstances of unusual or unjustified complexity;

(c) appears to have no economic justification or lawful objective;

(d) is made by or on behalf of a person whose identity has not been established to the satisfaction of the person with whom the transaction is made and

(e) gives rise to suspicion for any other reason.

For further details on how to identify and report a suspicious transaction, please refer to the FIU current Guidance Note No 3, mentioned above.

The offence for failing to report an STR is set out under section 19 of the FIAMLA. The penalty is a fine not exceeding one million rupees and imprisonment for a term not exceeding 5 years.

6.1 Lodging a suspicious transaction report

The procedure to lodge a suspicious transaction report is laid down under section 15 of the FIAMLA which requires that every report shall be lodged with the FIU; the report shall be in such a form as approved by the FIU; and the report includes;

- the identification of the party or parties to the transaction;
- the amount of the transaction, the description of the nature of the transaction and all the circumstances giving rise to the suspicion;
- the business relationship[5] of the suspect to the bank, financial institution, cash dealer or member of a relevant profession or occupation
- where the suspect is an insider, whether the suspect is still affiliated with the bank, financial institution, cash dealer, or member of a relevant profession or occupation;
- any voluntary statement as to the origin, source or destination of the proceeds
- the impact of the suspicious activity on the financial soundness of the reporting institution or person;
- the names of all the officers, employees or agents dealing with the transaction

No report of a suspicious transaction shall be required to be disclosed or be admissible as evidence in any court proceedings. Further information on how STR's shall be reported may be found in the FIU's **Guidance Note No. 3** which is available on the FIU's website.

All employees in casino and gaming houses have an obligation to report information, particularly where they have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing, including criminal spend or financing of terrorism. In view of this, casino and gaming house operators are expected to have a framework in place

5 "business relationship" means an arrangement between a person and a reporting person, where the purpose or effect of the arrangement is to facilitate the carrying out of transactions between the person and the reporting person on a frequent, habitual or regular basis;

whereby:

- they ensure that employees are appropriately trained in their obligations, and in the requirements for making reports to their Money Laundering Reporting Officer.
- they must ensure that, employee report to the Money Laundering Reporting Officer where they have grounds for knowledge or suspicion that a person or customer is engaged in money laundering or terrorist financing; and
- the Money Laundering Reporting Officer (MLRO) considers such reports, and is able to determine whether it gives grounds for knowledge or suspicion.

There are numerous flags which may induce suspicion of ML/TF. Section 6 delineates further the traditional red flags which may constitute suspicious activity. Whilst not exhaustive, these typologies attempt to portray a set of contextual scenarios of typical ML/TF suspicious activity.

Upon knowledge or suspicion of ML/TF or criminal spend in one area of the business (for example, table games) is observed, the operator should monitor the customer's activity closer in other areas of the business (for example, gaming machine play) and report to the FIU, should these suspicions manifest further.

6.2 Request for Information by the FIU

Under Section 13(2) and section 13(3) of FIAMLA, the Director of the FIU may, having regard to the complexity of a case, request additional information from that person licensed to operate a casino and gaming house among others under the Gambling Regulatory Authority Act who submitted the suspicious transaction report or from any other reporting entity which is, or appears to be, involved in the transaction. The additional information shall, as soon as practicable but not later than 15 days, be furnished to the FIU.

If the casino or gaming house operator fail to supply any information requested by the FIU under section 13(2) or 13(3) of FIAMLA, they commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years as per section 19 of the FIAMLA.

6.3 Disclosure of Information

Confidentiality is a key success factor for the operations of an FIU. Under section 30(1) of the FIAMLA, the Director, every officer of the FIU, the Chairperson and members of the Board shall take an oath of confidentiality before they begin to perform their duties. They should maintain during and after their relationship with the FIU, the confidentiality of any matter relating to the relevant enactments. Section 30(2) of the FIAMLA further provides that no information from which an individual or body can be identified and which is acquired by the FIU in the course of carrying out its functions shall be disclosed except where disclosure appears to the FIU to be necessary to enable it to carry out its functions, or in the interests of the prevention or detection of crime, or in connection with the discharge of any international obligation to which Mauritius is subject. Any breach of this section shall be punishable by a fine not exceeding Rs1 million and to imprisonment for a term not exceeding 3 years.

The FIU takes all the necessary precautions to protect the identity of the person reporting the suspicious transaction when disclosing the information to law enforcement or other competent authorities. As regards physical security, the FIU Mauritius has a well-defined architecture covering access control. Confidentiality of IT-information and databases is well-preserved by IT Security Policies and Procedures.

6.4 Tipping off

Following the submission of a suspicious transaction report to the FIU, Section 16 (1) of FIAMLA prevents that any person licensed to operate a casino and gaming house under the Gambling Regulatory Authority Act 2007, from informing anyone, including the customer, about the contents of a suspicious transaction report or even discloses to him that he/she has made such a report or information has been supplied to the FIU pursuant to the request made under section 13(2) or 13(3) of FIAMLA. An offence under this Act is punishable by a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

In such cases where the employee suspects that CDD will tip off the client, the employee should stop conducting CDD and instead file an STR with the FIU.

6.5 Requirements to cease transactions or terminate relationship

Where a casino and gaming house operator are unable to apply the required CDD measures in relation to a customer, the operator:

- must not carry out a transaction with the customer;
- must terminate any existing business relationship with the customer; and
- must consider whether they are required to report with the FIU.

7. TERRORIST FINANCING OFFENCES AND SANCTION SCREENING

7.1 Introduction

Terrorist organizations require funds to plan and carry out attacks, train militants, pay their operatives and to create propagandas on their causes. The UN Sanctions Act criminalizes the provision of monetary support for terrorist purposes through the United Nations Security Council Resolutions on targeted sanctions including financial sanctions, arms embargo and travel ban.

7.2 Extension of obligations

According to section 19H & K of the FIAMLA, a member falling under the purview of a regulatory body must ensure compliance with the UN Sanctions Act as well. The prohibition to deal with funds or other assets of a designated party or listed party applies to all persons including Casinos and Gaming Houses as delineated in section 23 of the UN Sanctions Act. In addition, section 24 of the UN Sanctions Act prohibits any person on executing transactions or making funds or other assets available to a designated party or listed party.

7.2.1 Reporting obligations

Where any casino and gaming house holds, controls, or has in his custody or possession any funds or other assets of a designated party or listed party, they shall immediately notify the National Sanctions Secretariat as per section 23(4) (UN Sanctions Act) about the:

i. details of the funds or other assets against which action was taken against;
ii. the name and address of the designated party or listed party; and
iii. details of any attempted transaction involving the funds or other assets, including-

- the name and address of the sender;
- the name and address of the intended recipient;
- the purpose of the attempted transaction;
- the origin of the funds or other assets and
- where the funds or other assets were intended to be sent.

The reporting obligations continue under section 25 of the UN Sanctions Act 2019 which states that a reporting person shall immediately verify whether the details of the designated or listed party match with the particulars of any customer.

7.2.2 Reporting of suspicious information

Pursuant to section 39 of the UN Sanctions Act, any information related to a designated party or listed party which is known to the reporting person should be submitted to the FIU in accordance with section 14 of the FIAMLA.

7.2.3 Internal controls

Section 41 of the UN Sanctions Act states that a reporting person shall implement internal controls and other procedures to enable it to effectively comply with their obligations under this Act

7.3 Sanction Screening

Casino and gaming house operators need to have the necessary policies, procedures and controls in place to monitor financial transactions so that payments are not made to designated persons, thereby preventing breaches to the UN Sanction Act 2019.

Casino and gaming house operators may wish to use the following official sources in order to screen and detect customers which are designated persons:

- the UN website (https://www.un.org/securitycouncil/content/un-sc-consolidated-list);
- the Interpol Red Notice (https://www.interpol.int/en/How-we-work/Notices/View-Red-Notices); and
- the Office of Foreign Assets Control (OFAC) website (https://www.treasury.gov/about/organizational-structure/offices/pages/office-of-foreign-assets-control.aspx)

7.3.1 Reporting Obligations

- Operators must immediately (i.e. without delay and not later than 24 hours), verify whether the details of the Listed Party match with the particulars of any of its customer;
- If there is a positive match, the operator must identify whether the customer owns any funds or other assets with it, including the funds or assets mentioned in section 23(1) of the UN Sanctions Act 2019;
- The operator institution is required to make a report to the National Sanctions Secretariat and the Gambling Regulatory Authority (GRA) where funds or other assets have been identified by it.
- A nil report must be submitted to the above authorities if no funds or other assets is identified.

Casino and gaming house operators should consider the likelihood of sanctioned persons using the casino's and gaming house's facilities. Operators are also urged to conduct regular screening of existing customers given that Sanctions lists are dynamic and can change frequently.

Contact details for the National Sanctions Secretariat:

National Sanctions Secretariat

Prime Minister's Office (Home Affairs)
Fourth floor
New Government Centre
Port Louis

Phone Number: (+230) 201 1264 / 201 1366
Fax: (+230) 211 9272
Email: nssec@govmu.org

8. NATURE AND SCOPE OF THE POWERS OF A REGULATORY BODY UNDER THE FIAMLA

8.1 Nature of the power

According to the First Schedule of the Financial Intelligence and Anti-Money Laundering Act 2002 (FIAMLA), the regulatory body for person licensed to operate a casino and gaming house is the Gambling Regulatory Authority (GRA) for Anti-money Laundering (AML) and Counter Financing Terrorism (CFT) & proliferation purposes.

8.2 Functions of the Regulatory Body

Pursuant to section 19G of the FIAMLA, the functions of a Regulatory Body are to:

i. supervise, monitor and give guidance to a member falling under its purview;
ii. cooperate with, and assist investigatory authorities;
iii. exchange information with investigatory authorities and supervisory authorities;
iv. assist and exchange information with overseas comparable regulatory bodies; and
v. undertakes and assist in research projects in order to identify the methods and trends of money laundering activities and the financing of terrorism and proliferation activities in Mauritius and in the region.

A regulatory body may enter into an agreement or arrangement for the exchange of information with an overseas comparable regulatory body while protecting the confidentiality of any information exchanged. A regulatory body may consult with, and seek such assistance from, any association or body representing a member or any other person as it may deem appropriate.

8.3 Scope of the powers of a Regulatory Body

According to section 19H of the FIAMLA, a regulatory body shall have such powers as are necessary to enable it to effectively discharge its functions and may, in particular –

f) issue guidelines for the purposes of combating money laundering activities and the financing of terrorism and proliferation activities;

g) give directions to a member falling under its purview to ensure compliance with this Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, and any regulations made and guidelines issued under those Acts;

h) require a member falling under its purview to submit a report on corrective measures it is taking to ensure compliance with this Act and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019, and any regulations made and guidelines issued under those Acts, at such intervals as may be required by the regulatory body.

i) With respect to a member falling under its purview, the regulatory body may apply any or all of the following administrative sanctions;

i. issue a private warning;
ii. issue a public censure;
iii. impose such administrative penalty as may be prescribed by the regulatory body;
iv. ban, where the regulatory body has licensed or authorised the member to conduct his business or profession, from conducting his profession or business for a period not exceeding 5 years; and
v. revoke or cancel a licence, an approval or an authorisation, as the case may be.
vi. Any person who fails to comply with a direction issued shall commit an offence and shall, on conviction, be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

It is noteworthy to highlight that a regulatory body may publish any of its decision or determination, or the decision of the Review Panel, or any other information the regulatory body may deem appropriate.

8.4 Request for information

As per section (19) (J) of the FIAMLA, a regulatory body may require a member falling under its purview to furnish any information and produce any record or document within such time as it may determine. Failing to comply with such requirement may constitute an offence punishable by a fine not exceeding one million rupees and to imprisonment for a term not exceeding 2 years.

8.5 Onsite Inspections

Section 19K of the FIAMLA states that a regulatory body may at any time-

Any person who intentionally obstructs and fails without any reasonable excuse to comply with any direction of the regulatory body shall commit an offence and be liable to a fine not exceeding one million rupees and to imprisonment for a term not exceeding 5 years.

i. audit and inspect the books and records of a member falling under its purview in order to verify that the member is compliant with the FIAMLA and the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019 (UN Sanctions Act); and
ii. direct orally or in writing the member to produce documents or material that is relevant to inspection.

Additionally, any person who destroys, falsifies, conceals or disposes of, or causes or permits the destruction, falsification, concealment or disposal of, any document, information stored on a computer or other device or other thing that the person knows or ought reasonably to have known is relevant to an onsite inspection or investigation, shall commit an offence and shall, on conviction, be liable to a fine not exceeding 5 million rupees and to imprisonment for a term not exceeding 10 years.

8.6 Directions by Regulatory Body

By virtue of section 19L of the FIAMLA, a regulatory body may give written directions to its member where he has reasonable cause to believe that a member who falls under its purview has failed or is failing to comply with the requirements under the FIAMLA and the UN Sanctions Act or is engaging in money laundering and the financing of terrorism and proliferation activities.

The regulatory body may take any of these actions-

i. remove or take steps to remove any specified employee from office;
ii. ask the member falling under its purview to refrain from doing a specified act;

iii. ensure that a specified employee does not take part in his management or conduct except as permitted by the regulatory body;
iv. appoint a specified person to a specified office for a period specified in the direction;
v. implement corrective measures and reports on the implementation of the corrective measures; and
vi. revoke a direction and notify accordingly its member.

Non-compliance with the direction of a regulatory body is punishable by 5000 rupees per day under section 19M of the FIAMLA. In addition, a person who knowingly hinders or prevents compliance with a direction may be liable to a fine not exceeding one million rupees and a term of imprisonment not exceeding 5 years.

8.7 Administrative sanctions

Where a regulatory body has reasonable cause to believe that a member falling under its purview has contravened the FIAMLA and/or the UN Sanctions Act, it is empowered to impose administrative sanctions under section 19N of the FIAMLA. Details of the Administrative Sanctions can be found at section 19H (1) (d) FIAMLA.

8.8 Compounding of offences

The regulatory body may with the consent of the Director of Public Prosecutions (DPP) compound any offence committed under the FIAMLA and the UN Sanctions Act as per section 19P of the FIAMLA.

Where the DPP does not give his consent to compound the offence or the person does not agree to the compounding of the offence, the regulatory body may, with the consent of the DPP, refer the matter to the police.

8.9 Review Panel

Section 19Q of the FIAMLA caters for the establishment of a Review Panel which will be responsible to review a decision of a regulatory body to impose an administrative sanction under section 19N of the same Act.

Under section 19S of the FIAMLA, a member who is aggrieved by the decision of the regulatory body, may within 21 days of the decision of the regulatory body, make an application to the Review Panel for a review of that decision.

Finally, the avenue for a judicial review of the determination of the Review Panel to the Supreme Court is made possible under section 19X of the FIAMLA.

CONTACT DETAILS

Gambling Regulatory Authority

Level 12 Newton Tower, Sir William Newton Street

Port-Louis

Republic of Mauritius

Telephone: (230) 260-2000

Fax: (230) 213-1250

Email: gra.admin@intnet.mu