TURKS & CAICOS ISLANDS

GAMING CONTROL COMMISSION

To Combat Money Laundering, Terrorist Financing and Proliferation Financing

Guidance for All Gaming Establishments

First Edition

Issued on May 13, 2022

TABLE OF CONTENTS

The contents of the AML Handbook are divided into the following Chapters and sections:

TABLE OF CONTENTS

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Jurisdiction

The Turks and Caicos Islands Gaming Control Commission Guidance to Combat Money Laundering, Terrorist Financing and Proliferation Financing shall hereinafter be referred to as "The AML Guidance". This AML Guidance is issued pursuant to Section 169 of the Gaming Control Ordinance[1] which provides for the issuance of Guidance by the Gaming Control Commission as the Supervisor of a Designated Non-Financial Business and Profession (DNFBP) being the Casinos and the Gaming Sector. The AML Guidance applies to all licensees and registrants within the Gaming Sector of the Turks & Caicos Islands ("TCI"), and contains all of the guidance necessary to operate a framework for compliance under the Gaming Control Ordinance, Proceeds of Crime Ordinance ("POCO"), along with the Anti-Money Laundering and Preventions of Terrorist Financing Regulations ("AML Regulations"), and the Anti-Money Laundering and Preventions of Terrorist Financing Code ("AML Code") and any subsequent legislative amendments.

This Guidance has been written by the Gaming Control Commission ("the Commission") to assist gaming licensees and operators to understand the requisite processes and procedures and to be used as a resource for establishing and implementing best practices that should be undertaken in the battle against money laundering, terrorist financing and proliferation financing. Thus, contributing to the overall efforts of protecting the Turks & Caicos Islands Gaming sector from those who seek to partake in illegal activities.

Furthermore, this Guidance seek to compliment the legal and regulatory requirements within the Turks & Caicos Islands. Therefore, licensees must comply with the Gaming laws and Regulations that have been enacted to in the fight against Money Laundering ("ML"), Terrorist Financing ("TF"), and Proliferation Financing ("PF").

[1] **169.** (1) of the Gaming Control Ordinance states: "*The Commission may, from time to time and with a view to enabling any person to order his affairs in compliance with the provisions of this Ordinance, issue such guidelines as it considers appropriate for providing guidance—*
(a) in furtherance of its regulatory objectives; or
(b) on any matter relating to gaming operations.
(2) The failure of any person to comply with any of the provisions of a guideline issued under this section that applies to him shall not of itself render that person for that reason only liable to criminal proceedings but any such failure may, in any proceedings whether civil or criminal, be relied upon by any party to the proceedings as tending to establish or to negate any liability which is in question in the proceedings"

1.2 Application and Guidance

1.2.1 The AML Guidance applies to every relevant person, employee or gaming operator in respect of all its activities carried out in or through the TCI gaming industry. These include: casino operations, slot parlour, gaming route, electronic bingo, sports betting, internet gaming, lottery operations, gaming-related operations, charity gaming, or any other such categories which may be permitted under the Gaming Control Ordinance.

1.2.2. The AML Guidance is not intended to be read in isolation from other TCI relevant legislation or developments in international policy and best practice and, to the extent applicable, relevant persons and Gaming Operators need to be aware of, and take into account, how these aforementioned matters may impact on the day-to-day operations within the gaming sector.

1.3 Responsibility for compliance with the AML Guidance

1.3.1 All gaming establishments are responsible for establishing, maintaining and monitoring the AML policies, procedures, systems and controls and compliance with applicable AML legislation.

1.3.2 (1) In carrying out their responsibilities under the AML Guidance, all businesses, its Senior Management and MLRO (as the case may be) must exercise due skill, care and diligence.

(2) Nothing in this Guidance precludes the Commission from taking enforcement action against any person, including any one or more of the following persons, in respect of a breach of the any legislation which regulates the Gaming Sector:

(a) any operator of a gaming establishment

(b) members of Senior Management; or an Employee of a gaming operations establishment.

1.4 Culture of Compliance

1.4.1 To promote and foster a culture of compliance, casinos, lotteries and relevant slot parlours gaming machine operators and other gaming establishments should allocate resources to improve AML compliance. These measures include:

(1) Establishing a system of internal controls and policies and procedures to assure ongoing compliance with AML requirements.

(2) Ensuring independent testing of AML compliance, of a scope and frequency that matches the ML/TF risks present.

(3) Training personnel, as warranted for individual jobs, in the identification of unusual financial transactions or suspicious transactions or activities, in the recording and aggregation of currency transactions, and all legal requirements and the Sector's compliance policies and procedures.

(4) Designating an individual or individuals responsible for assuring day-to-day AML compliance at all venues.

(5) Providing adequate resources to compliance functions.

2. OVERVIEW AND PURPOSE OF THE AML GUIDANCE

2.1 Gaming establishments have a responsibility to uphold the statutory objectives set out in the **Gaming Control Ordinance** and its subsequent regulations as well as the AML Codes and AML Regulations. Further, gaming licensees shall endeavour to prevent gambling from being a source of crime or disorder, being associated with crime or disorder or being used to support crime. Hence, the purpose of this document is to provide a resource for gaming licensees in establishing and implementing adequate procedures that meet the industry best practices standards while protecting the gaming industry and the broader financial system from money launderers and those involved in illegal activities.

2.2 Turks & Caicos Criminal Law: Proceeds of Crime Ordinance ("POCO")

Section 127 of POCO imposes an obligation on a person who knows or suspects or have reasonable grounds for knowing or suspecting that someone else is engaging in money laundering, terrorist financing or another criminal activity[2].

A person who does not report this information as it becomes known to them, commits an offence. Gaming establishments are also reminded that:

[2] Section 127(1) Proceeds of Crime Ordinance

(a) the failure to report suspicions of money laundering, terrorist financing or any other criminal activity;

(b) "tipping off"[3]; and

(c) assisting in the commission of Money laundering, terrorist financing or any other criminal activity

may each constitute a criminal offence that is punishable under the laws of the Turks & Caicos Islands.

2.3 Section 127(1) of POCO mandates that a person who knows or suspects that another person is engaging in money laundering or terrorist financing, must promptly make a disclosure to the relevant Money Laundering Reporting Officer (MLRO) if he makes the disclosure in the course of his employment and in accordance with the procedures established by his employer for this purpose, or to the Financial Intelligence Agency ("FIA").

Financial Action Task Force Standards

. The Financial Action Task Force (the "FATF") is an inter-governmental body whose purpose is the development and promotion of international standards to combat ML/TF & PF.

The Caribbean Financial Action Task Force (the "CFATF") is also an inter-governmental body which is a division of the FATF for the purpose implementing and promoting of international standards of combatting ML/TF & PF within the Caribbean region.

3. INTERPRETATION AND TERMINOLOGY

3.1 Glossary for AML Guidance on the term "customer" or "patron"

1. The point at which a person becomes a customer or patron will vary from business to business. However, the Commission considers that it would usually occur at or prior to the business relationship being formalized, for example, by the signing of a client agreement or the acceptance of the terms by the customer.

[3] Tipping Off is disclosing or providing hints to another directly or indirectly, information that is likely to prejudice an investigation. Tipping Off also occurs when someone discloses that a suspicious transaction report or related information is being filed with the FIA. See also Section 129 of POCO

The Commission does not consider that a person would be a customer of a gaming establishment merely because such person receives marketing information from a gaming establishment; or where a gaming establishment refers a person who is not a customer to a third party.

The Commission also considers that a Counterparty would generally be a customer for the purposes of the AML Guidance and would therefore require a gaming operator to undertake CDD on such a patron. However, this would not include a counterparty in a transaction undertaken on a regulated exchange; nor would it include suppliers of ancillary business services for consumption by the gaming operator such as cleaning, catering, stationery, IT or other similar services.

3.2.1 The following terms and abbreviations bear the following meanings for the purposes of this guidance.

Abbreviations

AML/ CFT/PF	Anti-Money Laundering/ Countering the Financing of Terrorism/Proliferation Financing
BO	Beneficial Owners
CDD	Customer Due Diligence
CFATF	Caribbean Financial Action Task Force
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FI	Financial Institution;
FIA	Financial Intelligence Agency
FSC	Financial Services Commission
GCC	Gaming Control Commission
GCO	Gaming Control Ordinance,
GE	Gaming establishment
ICS	Internal Control Standards
KYC	"Know Your Customer" requirements

ML	Money Laundering
MLRO	Money Laundering Reporting Officer
PEP	Politically Exposed Person
PF	Proliferation Financing
POCO	Proceeds of Crime Ordinance
PTO	Prevention of Terrorism Ordinance
RBA	Risk-based approach
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TCI	Turks & Caicos Islands
TF	Terrorist Financing
UK	**United Kingdom**
UN	**United Nations**

3.2.2 The following terms, interpretations and definitions are provided for the purposes of this Guidance in accordance with Gaming Control Ordinance.

Definitions

Applicant	A person who applies to a licensing authority for a license under the Gaming Control Ordinance (or any subsequent legislative amendments);
Casino	Refers to either a Class A- integrated operator or Class B- standalone Casino;
Cheating	To alter the result of a gambling game, the element of chance, the operation of a machine used in gambling game, or the method of selection of criteria as prescribed in GCO;
Chips	Any tokens used instead of money for the purpose of gaming and includes any voucher or other instrument that has a fixed dollar wagering value;
Customer	An individual who participates in gaming within a gaming facility; also known as a patron;

Gaming Establishment	Casino operations, slot parlour, gaming route, electronic bingo, sports betting, internet gaming, lottery operations, gaming-related operations, charity gaming, or any other such categories which may be permitted under the Gaming Control Ordinance.
Gambling Offence	A contravention of any gaming requirements under the GCO; and includes cheating at a game, submitting false information on a gaming application, operating an illegal game, and fraud;
Gaming Employee	Any employee of a gaming operator, gaming establishment or management company, but does not include a key employee;
Gaming Facility	The premises on which games licensed and regulated under GCO are conducted;
Gaming Operator	The holder of a license to operate games regulated under GCO;
Financial Institution	A company which carries on a banking business including banking business carried on by a trust company;
Key Employee	Any executive, employee, or agent of a gaming operator license or management company licensee having the power to exercise significant influence over decisions concerning any part of the operations of such licenses including any subsequent legislative recommendations prescribed in GCO.
Key Person	An entity that is a holder of any direct or indirect legal or beneficial publicly traded or privately held interest whose combined direct, indirect, or attributed publicly traded interest is 5% or more or privately held interest is 1% or more in an applicant or licensee or in a key business entity of an applicant or licensee; or any subsequent recommendations prescribed in GCO;
Licensee	A person who is issued a licence under GCO;
Patron	opens a patron account with a gaming operator; or is involved in a

cash transaction with a gaming operator within its facility, whether or not that person participates in gaming in the gaming facility.

4. GENERAL COMPLIANCE REQUIREMENTS

4.1 General requirements

4.1.1 A gaming establishment must institute and maintain effective AML/CFT policies, procedures, systems and controls to prevent opportunities for ML/TF or PF, in relation to the gaming establishment and its activities.

2. A gaming establishment's AML/CFT policies, procedures, systems and controls must:

(a) ensure compliance with Turks & Caicos Islands ("TCI") AML/CFT Legislation;

(b) enable suspicious activities and transactions to be detected and reported;

(c) ensure the gaming establishment is able to provide an appropriate audit trail of a transaction; and

(d) ensure compliance with any other obligation in this Guidance.

(3) A gaming establishment must take reasonable steps to ensure that its employees comply with the relevant requirements of its AML/CFT policies, procedures, systems and internal controls.

(4) A gaming establishment must review the effectiveness of its AML/CFT policies, procedures, systems and controls annually.

(5) The review process to be undertaken must include:

(a) internally by its internal audit or compliance function; or

(b) by a competent firm of independent auditors or compliance professionals.

(6) The review process required under paragraph 4.1.1(4) must cover the following:

(a) a sample testing of customer documentation relevant to an assessment of the adequacy of the customer risk assessment or CDD performed by the gaming establishment;

(b) an analysis of all SARs to highlight any area where procedures or training may need to be enhanced; and

(c) a review of the adequacy of the level of responsibility and oversight of the gaming establishment in ensuring it has implemented and maintained adequate controls.

4.2 Notification

4.2.1 A gaming establishment must inform the Commission in writing as soon as possible if, in the course of its activities, it suspects or becomes aware or suspicious that a patron of its business:

(a) receives a request for information from a regulator or agency in another jurisdiction responsible for AML/CFT or Financial Sanctions regarding enquiries into potential ML/TF/PF or Financial Sanctions breaches;

(b) becomes aware, or has reasonable grounds to believe, that the following has or may have occurred in or through its business:

(i) ML/TF or PF, contrary to relevant TCI AML/CFT Legislation, policy the AML/CFT Guidance

(ii) a breach of Financial Sanctions; or

(iii) acts amounting to bribery

4.3 Record keeping

4.3.1 A gaming establishment must, where relevant, maintain the following records:

(a) a copy of all documents and information obtained in undertaking initial and on-going CDD or due diligence on patrons;

(b) records, consisting of the original documents or certified copies, in respect of the customer business relationship, including:

(i) business correspondence and other information relating to a customer's account;

(ii) sufficient records of transactions to enable individual transactions to be reconstructed; and

(iii) internal findings and analysis relating to a transaction or any business, if the transaction or business appears unusual or suspicious, whether or not it results in a SAR;

(c) SARs and any relevant supporting documents and information, including internal findings and analysis;

(d) any relevant communications with the Commission;

(e) any other matter that the gaming establishment is expressly required to record under this Guidance, for at least five years from the date on which the notification or report was made, the business relationship ends or the transaction is completed, whichever occurs last.

4.4 Co-operation with the Gaming Control Commission

4.4.1 A gaming establishment must:

(a) be open and cooperative in all its dealings with the Regulator; and

(b) ensure that any communication with the Regulator is conducted in writing and in the English language.

4.5 Employee disclosures

4.5.1 A gaming establishment must ensure that it does not prejudice an employee who discloses any information regarding ML/TF/PF to the Commission in the prevention of ML/TF/PF.

5. THE LICENSING REGIME

5.1 Introduction

All individuals or entities seeking to be employed within the gaming industry or seeking to conduct business within the gaming industry in the TCI must be licenced. Essentially, no person in the TCI, without the appropriate licence, shall conduct or permit the conduct or be directly or indirectly involved in the operation of any gaming business or establishment.

5.1.2 Background Checks and Investigations

The purpose of a probity investigation is to determine whether such applicants are suitable or deemed "fit and proper" to receive a licence pursuant to Section 32 of the Gaming Control Ordinance. Therefore, to qualify for a licence, a natural person must be a fit and proper person whose character, integrity, honesty, prior conduct, regard for the law, reputation, habits and associations do not pose a threat to the health, safety, morals, good order and general welfare of the inhabitants of the TCI and to the provisions of the Gaming Control Ordinance. The investigation must be extensive, because it is the first step to ensure a business or individual is fit to participate in the gaming industry.

As such, the investigations can encompass but are not limited to an examination of the personal history of the applicant and the ultimate beneficial owners of any corporation, police reports, educational, financial and character reference verification, neighbourhood checks, past and present employment checks, and an interview. The Commission can also produce detailed reports with the assistance of local and external enforcement agencies and other gaming regulatory bodies in various jurisdictions. At the conclusion of investigations, licensees may be issued with or without conditions, or an application may be rejected. Conducting background checks of individuals prior to their participation in the gaming industry is the first step the Commission takes in ensuring that gaming is conducted in an honest, competitive environment, free of any criminal element.

5.2 TYPES OF LICENCES

Pursuant to Section 41 of the Gaming Control Ordinance, the following are the categories of licenses which can be issued:

1. **Class A:** Integrated Resort Casino Operator;
2. **Class B:** Stand-alone casino operator's licence;
3. Slot Parlour Licence;
4. Gaming Route Licence;
5. Electronic Bingo Licence;
6. Sports Betting Licence;
7. Internet Gaming Operator's Licence;
8. Lottery Operator's Licence;
9. Proxy Lottery Operator's Licence;
10. Suppliers Licence;
11. Route Operator Licence;
12. Gaming-Related Vendor Licence;
13. Charitable Gaming or Special Game of Chance Licence;
14. International Market Agent Operator's Licence;
15. International Market Agent Representative Licence; and
16. Other category of licences as may be prescribed.

5.2.1 Gaming Control Ordinance 2018 (GCO)

For further references and characteristics on the above licences, please refer to Part III of the Gaming Control Ordinance.

5.3 Gaming Establishments Internal Investigation

5.3.1 Prior to submission of a Key Employee or Key Person Licence application, a gaming establishment must conduct preliminary due diligence, to ensure that, at a minimum, the applicant is fit for office. The fee for such applications is non-refundable, even in cases where the applicant later withdraws the application or in cases where the application is not approved.

5.4 Application Process

5.4.1 Key Employee Licence/ Key Person Licence

1. The first step in applying for a Key Employee or Key Person Licence is that the applicant must have been offered employment by the gaming establishment.

2. Subsequent to being offered a position by the gaming establishment, the applicant is required to complete a requisite "**Personal Declaration Form"**. The Form should be carefully completed in its entirety, inclusive of all requisite signatures and documents to support the application. Failure to do so can delay the processing of the application or in extreme cases, result in denial. The following documents are required:

a. Duly completed Personal Declaration Form
b. Two (2) identical passport size photos signed and dated by a Notary Public or Justice of the Peace on the back. Photo shall not be older than six (6) months old
c. Copies of all relevant pages of the applicant's passport ensuring that all visa, work permit and permanent residence entries are clearly legible. Non-Turks & Caicos Islanders should provide proof of citizenship and right to work (Spousal Permit, Permanent Residence Certificate)
d. Original Criminal Record Character Certificate (not more than six (6) months old
e. Original Finger Print Certificate
f. A certified copy of Turks & Caicos Islander Status Card (if applicable)

g. Certified copy of Birth Certificate
h. Certified copy of Marriage Certificate or Divorce Decree where applicable.
i. Three (3) Original Character References (signed and dated not more than six (6) months old inclusive of the contact details of the persons giving the character reference.
j. Proof of Residence verification i.e. (Lease, or current Utility Bill not older than three months)
k. Certified Educational Verification with a copy of Resume (attached certified copies of all tertiary qualifications)
l. Business affiliations and prior gaming licences
m. Proof of ownership of all vehicles
n. Bank Statements for the most recent three-month period for each bank account listed.
o. A Bank reference letter
p. If applicable, Copy of Income Tax Returns for the three (3) years preceding the date of the application. If the applicant was not required to file income tax returns for three (3) years directly preceding the date of this application, the applicant shall provide proof of one's income for the previous three (3) months as well as copies of one's salary (pay-slip) for the past three months.
q. If applicable, supporting court documents
r. If ever declared legally insolvent, bankrupt, or having filed a petition for any type of bankruptcy of insolvency under any Bankruptcy or Insolvency Legislation, one must provide a certified and legible copy of the Court Order.
s. Notarized Authorization Form

3. Prior to submission of the application form, the Applicant must bear in mind that the Commission is assessing his/her character, honesty, and integrity, therefore the Applicant is to ensure the following:

a. Every question has been answered completely and truthfully
b. That he/she has followed all instructions on each application
c. All requisite documents are attached
d. That he/she has retain a copy of his/her records/documents
e. The Personal Declaration Form is the originally signed document

Note: All Forms are available on request from the Office of the Gaming Control Commission

5.4.2 For Consideration

THE FOLLOWING SHOULD BE NOTED:

1. Having a criminal record may affect the outcome of your application, particularly if one has been convicted within the **past ten (10) years** in any country of any criminal activity.
2. Once approved, all licences are valid for a period of one (1) year.
3. Full probity is conducted during the first year (initial application) and limited probity is conducted during the second and third year. Full probity shall include requesting and verifying all information outlined in paragraph 5.4(2) & (3) above.
4. All renewal application forms are due for submission to the Gaming Commission ninety (90) days in advance of the Licensees expiration date of the licence.
5. As a means of ensuring compliance, failure to submit all requisite documents and/or to avail oneself for all scheduled interview or appointments, the Commission reserves the right to place such applicants on a **"Stop List"**. This means that the individual will no longer be able to function in the *approved or requested* capacity in the gaming establishment.

5.4.3 Renewal Process

1. With regards to limited probity for a Gaming Operator/Key Employee, the operator must submit either an **"Application to Renew a Gaming Employee Licence"** or the **"Application to Renew a Key Employee Licence"** on behalf of the applicant to the Commission employee ninety (90) days in advance of the expiration date. The application should be accompanied by a police certificate not more than six (6) months old and a signed and notarized **"Authorization for Examination and Release of Information Indemnification"** form. Further, documented proof of any personal information should be submitted as a means of updating the relevant file (e.g., new Passport, Driver's Licence, TCI Islander Status Card, Work Permit – where applicable).
2. It should be noted that at any time during the course of the year, the Commission reserves the right to call a licensee in, if deemed necessary in order to verify any information pertaining to him/her. This includes information from secondary sources. **The Commission reserves the right to revoke a license at any time, if deemed necessary.**

6. APPLYING A RISK-BASED APPROACH TO THE GAMING SECTOR

6.1 The risk-based approach

6.1.1 A gaming establishment must:

(a) assess and address its AML/CFT risks under the AML Guidance by reviewing the risks to which the gaming establishment is exposed as a result of the nature of its business, customers, products, services and any other matters which are relevant in the context of ML/TF & PF; and

(b) ensure that any risk-based assessment undertaken for the purposes of complying with a requirement in the AML Guidance is:

(i) objective and proportionate to the risks;

(ii) based on reasonable grounds;

(iii) properly documented; and

(iv) updated at appropriate intervals.

Guidance

1. Paragraph 6.1.1 requires a gaming establishment to adopt an approach to AML/CFT which is proportionate to the risks. This is called the "risk-based approach" ("RBA"). The Commission expects the RBA to be a key part of the gaming establishment's AML/CFT compliance culture and to cascade down throughout the rest of the gaming sector.

2. In implementing the RBA, a gaming establishment is expected to have in place processes to identify, assess, monitor, manage and mitigate ML/TF & PF risks. The general principle is that where there are higher risks of ML/TF/PF, a gaming establishment is required to take enhanced measures to manage and mitigate those risks, and that, correspondingly, when the risks are lower, simplified measures are permitted. Simplified measures are not permitted where there is a suspicion of ML/TF/PF.

3. In determining which situations can place gaming establishments in peril; in conducting a risk assessment an analysis can be done of standard risk categories utilized by the FATF namely:

- Country or Geographic Risk
- Customer Risk

- Transaction Risk

4. A key to the conduct of any risk assessment is to adopt an approach which facilitates a distinction between the extent of different risks to assist with prioritization if mitigation efforts. The risk assessment process should consist of the following standards:

- **Identification:** This stage seeks to develop an initial list of potential risks or risk factors when combating ML/TF/ PF.
- **Analysis:** This stage involves consideration of the nature, sources, likelihood, impact and consequences of the identified risks or risk factors. The aim of this stage is to gain a comprehensive understanding of each of the risks. Risk analysis can be undertaken with varying degrees of detail, depending on the type of risk, the purpose of the risk assessment, and the information, data and resources available.
- **Evaluation:** This stage involves assessing the risks analysed during the previous stage to determine priorities for addressing them, taking into account the purpose established at the beginning of the assessment process. These priorities can then contribute to the development of a strategy for the mitigation of the risks.

7. BUSINESS RISK ASSESSMENT

7.1 Assessing business AML risks

7.1.1. The implementation of a risk-based approach is highly dependent on the gaming establishment's business risk assessment. Gaming licensees are in the best position to identify those areas of their operations that present the greatest risks of ML/TF & PF and therefore those which should be the focus of their attention. Thus, gaming licensees are required to:

(a) take appropriate steps to identify and assess ML/TF/PF risks to which its business is exposed, taking into consideration the nature, size and complexity of its activities;

(b) when identifying and assessing the risks in (a), take into account, to the extent relevant, any vulnerabilities relating to:

(i) its type of customers and their activities;

(ii) the countries or geographic areas in which it does business;

(iii) its products, services and activity profiles;

(iv) the complexity and volume of its transactions;

(v) the development of new products and business practices including new delivery mechanisms, channels and partners;

(vi) the use of new or developing technologies for both new and pre-existing products and services;

(vii) its employees

(viii) unusual transactions

(ix) transactions outside of the customer's normal activity

(x) transactions arising from higher risk counties as outlined in the

FATF recommendations.

(c) monitor information held relative to:

(i) Customer's Financial Habits

(ii) Customer's Gambling Habits

(d) give due consideration to the ML/TF/PF risks posed by their business-to-business relationships including any third-parties they contract with. The assessment of these risks is based, among other things, on the risks posed to the operator by transactions and arrangements with business associates and third-party suppliers such as gaming product suppliers or payment providers and processors, including their beneficial ownership and source of funds. Effective management of third-party relationships should assure gaming establishments that the relationship is a legitimate one, and that they can evidence why their confidence is justified.

(e) must also record in writing and detail actions that are taken in their pursuit to achieve compliance with the gaming laws particularly as it relates to the execution of their business risk assessments.

7.2 AML/CFT Systems and Internal Controls

7.2.1. Prior to commencing licenced operations, a gaming establishment must:

(a) establish and maintain effective policies, procedures, systems and controls to prevent opportunities for ML/TF/PF;

(b) develop a policy and submit for the Commission's approval, written internal controls standards which set forth controls that are in place to effectively manage and minimize gaming related risks.

(c) also, gaming establishments shall set forth controls to be implemented by it to ensure:

(i) the integrity of its operation;

(ii) that gaming devices, documents and information are properly controlled and safeguarded;

(iii) that unaccounted drop is secured;

(iv) that financial and other gaming-related records are accurate and reliable;

(v) that gaming-related transactions are performed with the necessary authorization;

(vi) that gaming-related transactions are recorded in sufficient detail to ensure the proper reporting of gaming revenue, taxes and other fees due.

(vii) that appropriate measures and procedures are in place to ensure compliance with all applicable provisions of the **Proceeds of Crime Ordinance and its accompanying subsidiary AML Regulations and AML Code, Gaming Control Ordinance, Financial Intelligence Ordinance, Prevention of Terrorism Ordinance** and any other applicable Legislation within the TCI, and

(viii) that gaming-related functions, duties and responsibilities are appropriately segregated and performed in accordance with international best practices by competent and appropriately qualified employees.

7.2.2. Further, the internal control systems developed by Gaming Establishments, shall describe programs which were developed by the licensee, having regard to its business risk assessment to ensure that it has such policies, procedures and controls as are appropriate and effective for the purposes of forestalling, preventing and detecting money laundering, terrorist financing and proliferation financing. Essentially, gaming establishments' internal control procedures which are compiled pursuant to the licensees' business risk assessment shall include information such as:

a. Applicable internal policies, procedures, and controls, including its policy for reviewing at appropriate intervals its compliance with the requirements of regulations;
b. Arrangements to manage compliance;

c. Screening practices when recruiting relevant employees;
d. Ongoing employee training program;
e. Audit function to test its systems;
f. Measures taken to keep abreast of and guard against the use of technological developments and new methodologies in ML/TF/PF financing schemes;
g. Patron identification and verification systems; and
h. Ongoing due diligence of the patron relationship.

7.2.3. Moreover, gaming establishments are required to regularly review their business risk assessment so as to keep it up to date. Gaming Establishments shall also seek approval from the Commission, where a change is required to its internal control procedures based on the review.

7.2.4. Furthermore, prior to registering a patron, or as soon as reasonably practicable thereafter; gaming establishments are required to undertake a risk assessment in respect of that patron. Additionally, the risk assessment of the patron shall also be regularly reviewed so as to keep it updated. This is done to ensure that the business has not become susceptible to new methodologies of money laundering, terrorist financing or proliferation financing. Notably, the review period has to take into account the size, nature, and complexity of the licensee's gambling offering; its registered customers, and the way it provides its services.

7.3 Signature Requirement for Gaming Establishments

7.3.1 An organizational structure should be in place for each gaming establishment's licensee and maintained consisting of Executive Management, Departments, Employee levels, and Job Responsibilities to ensure proper segregation of duties within each independent division of the organization. A clear chain of command should also be indicated to ensure continuous authorization and supervision of gaming and related activities. In this regard, a *signature listing* is required to ensure proper operation and effective supervision of gaming and related activities. Subsequently, persons deemed to be directly involved in the activities performed under the principal licence has, or will have, the express, implied or reasonably incidental authority to

perform any activity in respect of the gaming operations of the principal licence holder, which may reasonably enable the person on whom such authority is conferred -

a. To manipulate or alter a selection of criteria which determine the result of any game on which wagering is accepted;
b. To engage or participate in cheating, as prescribed in **Sections 153 - 160** of the Gaming Control Ordinance; or
c. To misrepresent to any authority, the tax liability of the licence holder,

7.3.2 For that reason, signatures are required by all key and gaming employees in the execution of their duties.

7.3.4 Signatures shall -

a. At a minimum, be the signatory's usual mark used to represent him or her.
b. Be immediately adjacent to or above the clearly printed or pre-printed name, title of the signer and his certificate number issued by the Commission.
c. Indicate that the signatory has prepared forms, records, and documents, and/or authorized, observed, and/or participated in a transaction to a sufficient extent to attest to the accuracy of the information recorded thereon, in conformity with the gaming regulations and the Licensees' system of accounting and internal controls, and
d. Indicate that if the signatory is required by the relevant legislation to count or observe the count of gaming chips that such count was made by breaking down stacks of chips to show each denomination and making a proper record of it.

7.3.5 Signature records shall be prepared for each gaming and key employee required to sign or initial forms, records, and documents and shall include specimens of signatures, initials and titles of signatories.

a. Such signature records shall be maintained on a dated signature card or sheet file, alphabetically by name, within a department.
b. The signature records shall be adjusted, on a timely basis to reflect changes in personnel.

c. Signature records shall be securely stored in the Accounting Department.

7.4 Summary of Minimum Internal Control Standards (ICS)

7.4.1. The ICS is used by the Commission to assess the procedures put in place by an operator prior to the operator being permitted to commence operations in order to comply with legislation applicable to the gaming industry and also to evaluate the operator's ongoing performance in complying with these procedures. An ICS should not be confused with a business risk assessment which is required specifically in relation to procedures relating to money laundering and the funding of terrorism and proliferation.

7.4.2. The Commission undertakes regular on-site inspections and off-site supervisory activities of the licensee's operations to assess whether the gaming licensee is conducting its business in a controlled manner, in conformity with the applicable laws regulation, and policies and to assess the correct application of the procedures documented in the approved ICS, and whether the gaming licensee's current approved ICS remains relevant and appropriate to its' business. The licensee must therefore ensure all operational changes are addressed in the ICS, and secure the Commission's formal approval prior to amending or implementing any such change in policy, procedures, or standards as contained in an approved ICS. Failure to comply with the approved ICS may result in the Commission enforcing any applicable penalties in accordance with the GCO.

8. RISK BASED CUSTOMER DUE DILIGENCE

8.1 Requirement to undertake Customer Due Diligence

In accordance with Regulation 11 of the AML Regulations as prescribed in POCO:

1. A key statutory requirement is to make checks on patrons, which can otherwise be described as Customer Due Diligence "CDD". CDD information comprises the facts about a patron that would enable a gaming establishment to assess the extent to which the patron exposes the gaming licensee to a range of risks; particularly those related to ML/TF/PF.
2. Gaming establishments must apply CDD measures it they:
    a. Establish a business relationship
    b. Suspect ML/TF/PF

c. Doubt the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification
d. Carry out an occasional transaction that amounts to $3,000 (USD) or more, whether the transaction is executed in a single operation or in several operations which appear to be linked.

3. Nonetheless, whether or not a business relationship with a patron has been established or there is no suspicion of ML/TF/PF; CDD measures should still be undertaken.
4. Gaming establishments must also apply CDD measures:
    a. At appropriate times to existing customers on a risk-based approach
    b. When the establishment becomes aware that the circumstances of an existing patron relevant to its risk assessment for that patron have changed.
5. As such, in determining when it is appropriate to apply CDD measures to existing patrons, gaming establishments must take into account the following, amount other things:
    a. Any indication that the identity of the patron has changed;
    b. Any transactions which are not reasonably consistent with the operator's knowledge of the customer;
    c. Any change in the purpose or intended nature of the operator's relationship with the patron;
    d. Any other matter which could affect the operator's assessment of the ML/TF/PF risk in relation to the customer.

8.2 Customer Due Diligence requirements

1. CDD measures consist of:
    i. Identifying the customer, inclusive of beneficial owners of legal entities, unless the identity of the customers is known to, and has been verified by, the gaming establishments.
    ii. Verifying the customer's identity, inclusive of beneficial owners of legal entities, unless the customer's identity has already been verified by the gaming establishment;
    iii. Assessing and, where appropriate, obtaining information on the purpose and intended nature of the business relationship.

2. The ways in which a gaming establishment meets the requirements for CDD and the extent of the measures it takes must reflect the risk assessment it has carried out, and its assessment of the level of risk arising in any particular case. This may differ from case to case.
3. In assessing the level of risk arising in a particular case, gaming establishments, must take account of factors including, among other things:
    i. The purpose of a patron account, transaction or business relationship
    ii. The amount deposited by a patron or the size of the transactions undertaken by the patron.
    iii. The regularity and direction of the business relationship.
4. Additionally, gaming establishments should satisfy themselves that the sources of information employed to carry out CDD checks are suitable to mitigate the fill range of risks to which they might be exposed, and these would include ML/TF/PF and social responsibility risks, such as those related to problem gaming. As such, gaming establishments must be able to demonstrate to the Commission that the extent of the CDD measures they take are appropriate in view of the risks of ML/TF/PF, including risks identified by the gaming establishments' risk assessment.

8.2.1 Identification and Verification

1. Notably, applying a CDD measures involves several steps. The gaming establishments are required to identify patrons and then verify their identities. Identification of a patron means being told or coming to know of the patron's identifying details, such as their name and address. Verification means obtaining some evidence which supports this claim of identity. The gaming establishment identifies the patron by obtaining a range of information from the patron. The verification of the identity consists of the gaming establishment verifying some of this information against documents, data or information obtained from a reliable and independent source.

2. Identification of patrons consists of a number of aspects, including retrieving relevant identifying information such as the patron's name, current and past addresses, dare of birth, place of birth, physical appearance, employment and financial history, family circumstances, and other like information. Also, it would be beneficial gaming establishment to obtain information on a patron's source of funds and level of legitimate income, for example their

occupation. This information may assist a gaming licence with their assessment about whether a patron's level of gambling is proportionate to their approximate income, or whether it is suspicious.

3. Information about a patron's identity must then be verified through documents, data and information which come from a reliable and independent source. In this regard, it is generally considered good practice to require either:
    a. A government document which verifies either name and address, or name and date of birth; or
    b. A government document which verifies the patron's full name and another supporting document which verifies their name and either their address or date of birth.
4. Also, there are a number of processes detailed below which when used may increase the confident that there is no money laundering or terrorist financing concern associated with the patron:
    a. Validation of patron documents – certified copies of documents to validate name, address, date of birth and source of funds of the customer.
    b. Source of Funds – Confirm the immediate source from which the funds have derived.
    c. Source of Wealth – corroborate sustainable wealth that matches the customer's gambling profile. This may also overlap with responsible gambling considerations. Accurately identifying a customer's source of funds and source of wealth can be a complex process and one in which approaching a patron directly for relevant evidence may be a last resort.
5. Nonetheless, no method of verification, with documentary or electronic, can conclusively prove that a patron is who one may claim to be. However, the Commission expects gaming establishments to be reasonably satisfied, following appropriate inquiry, that patrons are who they claim to be.
6. Finally, patron verification is key in ensuring that gaming establishments can be satisfied that patrons are who they say they are and are not acting on behalf of anyone else and they do not feature on a PEP or UN or UK Sanctions list. Patron co-operation is vital to ensure that the right information is provided and verified and one way in which this is achieved is by making the patron verification process as easy and user-friendly as possible. This, patrons should be

notified that they must undergo a standard verification process before they can begin use the services of a gaming licensee.

8.3 Enhanced Customer Due Diligence for Gaming Establishments

8.3.1. The aim of Enhanced Due Diligence is to obtain a level of confidence that the account is not funded by the proceeds of crime or used to finance terrorism. Therefore, gaming establishments must apply enhanced CDD measures and enhanced ongoing monitoring, in addition to the required CDD measures, to manage and mitigate the ML/TF/PF risks arising in the following scenarios:

- In any case identified by a gaming establishment or on information provided by the Commission to a gaming establishment as one where there is a high risk of ML/TF/PF;
- In any business relationship or transaction with a patron situated in a high-risk country as identified by the FATF, other international bodies, the TCI Government on the recommendation of the AMLC;
- In instances where the gaming establishment has determined that a customer or potential customer is a PEP, or family member or known close associate of a PEP;
- In any case where a gaming establishment discovers that a patron has provided false or stolen identification documentation or information and the gaming establishment proposes to continue to deal with the patron;
- In any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, and the transaction(s) have no apparent economic or legal purpose in any other case which, by its nature, can present a higher risk of ML/TF/PF.

8.3.2. Also, when assessing whether there is a high risk of ML/TF/PF in a particular situation, and the extent of measures which should be taken to manage and mitigate the risk, the gaming establishment must take account of the following risk factors, among other variables such as whether:

- The business relationship is conducted in unusual circumstances
- In the case of a casino, the customer is resident in a geographical area of high risk
- The product or transaction might favour anonymity

- The situation involves non-face-to-face business relationships or transactions (as in the case of slot parlours)
- Payments will be received from unknown or un-associated third parties of the patron
- New products and new business practices are involved, including new delivery mechanisms, and the use of new or developing technologies (such as virtual currencies) for both existing and new products
- In the case of casinos, the business relationship or transaction involves countries identified by credible sources (such as evaluations, detailed assessment reports or follow-up reports published by FATF, the International Monetary Fund, the World Bank, the organization for Economic Cooperation and Development or other international bodies or non-governmental organizations) as not having effective systems to counter ML/TF/PF or as not implementing requirements to counter ML/TF/PF that are consistent with the FATF recommendations.

8.3.3. The Commission mandates that gaming establishments also consider the following factors when assessing whether there is a high risk of ML/TF/PF:

- The patron transacts with significant amounts of cash;
- The patron provides false, forged or stolen identification, documentation upon establishing a business relationship;
- The patron transactions with multiple slot parlours;
- The product, service or transaction involves Ticket In/Ticket Out (TITO) or similar technology.

8.3.4. Notwithstanding the above-mentioned factors, in assessing whether there is a high risk of ML/TF/PF, gaming establishments must bear in mind that the presence of one or more of the risk factors listed above may not always indicate that there is a high risk in a particular situation.

8.4 Ongoing Customer Due Diligence and Enhanced Due Diligence

8.4.1. When undertaking on-going CDD under paragraph 8.3.1(d), a gaming establishment must:

(a) monitor transactions undertaken during the course of its customer relationship to ensure that the transactions are consistent with the gaming establishment's knowledge of the customer, the business and risk rating;

(b) pay particular attention to any complex or unusually large transactions or unusual patterns of transactions that have no apparent or visible economic or legitimate purpose;

(c) enquire into the background and purpose of the transactions in (b);

(d) periodically review the adequacy of the CDD information it holds on customers and beneficial owners to ensure that the information is kept up to date, particularly for customers with a high-risk rating; and

(e) periodically review each customer to ensure that the risk rating assigned to a customer under paragraph *7.1.1(b)* remains appropriate for the customer in light of the ML/TF/PF risks.

8.4.2 A gaming establishment must apply an intensified and on-going monitoring programme with respect to higher risk transactions and customers.

Guidance

1. The customer identification process does not end at the time of establishing a business relationship with a customer or, where relevant, undertaking a specific transaction or business activity on behalf of a customer. Following the start of the customer relationship, a gaming establishment must ensure that all relevant evidence and information is kept up-to-date including, for example, the list of authorized signatories who can act on behalf of a corporate customer.

2. In complying with paragraph 8.6.1(d), a gaming establishment must undertake a periodic review to ensure that non-static customer identity documentation is accurate and up-to-date. A gaming establishment is expected to ensure that the information and the evidence obtained from a customer is valid and has not expired, for example when obtaining copies of identification documentation such as a passport or identification card. Examples of non-static identity documentation include passport number and residential/business address and, for a Legal Person, its share register or list of shareholders and directors.

3. A gaming establishment must undertake a review under paragraph 8.6.1(d) and (e) particularly when:

(a) the gaming establishment changes its CDD documentation requirements;

(b) an unusual transaction with the customer is expected to take place;

(c) there is a material change in the business relationship with the customer; or

(d) there is a material change in the nature or ownership structure of the customer.

4. The degree of the on-going due diligence to be undertaken will depend on the customer risk assessment carried out under paragraph 7.1.1.

5. A gaming establishment's transaction monitoring policies, procedures, systems and controls, which may be implemented by manual or automated systems, or a combination thereof, are one of the most important aspects of effective CDD. Whether a gaming establishment must undertake the monitoring by means of a manual or computerized system (or both) will depend on a number of factors, including:

(a) the size and nature of the business and customer base; and

(b) the complexity and volume of customer transactions.

6. As part of a gaming establishment's ongoing monitoring and EDD processes, gaming establishments are expected to not only detect and report on suspicious transactions but to keep client identification information up-to-date when circumstances indicate that there has been a change, and to continuously re-evaluate customer risk based on a customer's activities and transactions.

7. If a customer does not provide proper identification and/or the required information, or if the gaming establishment cannot verify a customer's information, or if there are clear indications of fraud, the gaming establishment must document the incident, and file a ***suspicious activity report (SAR) with the FIA***, report the incident to authorities, and determine whether it should discontinue providing further services or engaging in additional transactions with the customer.

8.4.3 A gaming establishment must review its customers, their businesses, and transactions, against the UN and UK Sanctions Lists when complying with paragraph 8.4.1(d).

8.5 Failure to conduct or complete Customer Due Diligence

8.5.1. Where, in relation to a customer, a gaming establishment is unable to conduct or complete the requisite CDD in accordance with paragraph 8.1.1 it must, where appropriate:

(a) not carry out a transaction with or for the customer through a bank account or in cash;

(b) not open an account or otherwise provide a service;

(c) not otherwise establish a business relationship or carry out a transaction;

(d) terminate or suspend any existing business relationship with the customer;

(e) return any monies or assets received from the customer; and

(f) consider whether the inability to conduct or complete CDD necessitates the making of a SAR under paragraph 13.3.1(c).

(2) A gaming establishment is not obliged to comply with (1)(a) to (e) if:

(a) to do so would amount to "tipping off" the customer, in breach of any AML Legislation; or

(b) the FIA directs the gaming establishment to act otherwise.

Guidance

1. In complying with paragraph 8.5.1(1) a gaming establishment should apply one or more of the measures in (a) to (f) as appropriate in the circumstances. Where CDD cannot be completed to a significant degree, it may be appropriate not to carry out a transaction pending completion of CDD. Where CDD cannot be conducted, including where a material part of the CDD such as identifying and verifying beneficial owners cannot be undertaken, a gaming establishment should not establish a business relationship with the customer.

2. A gaming establishment should note that paragraph 8.5.1 applies to both existing and prospective customers. For prospective customers, it may be appropriate for a gaming establishment to terminate the business relationship before a product or service is provided. However, for existing customers, while termination of the business relationship should not be ruled out, suspension may be more appropriate depending on the circumstances, whilst further investigations are carried out. Whichever course of action is taken, the gaming establishment must be careful not to tip off the customer.

3. A gaming establishment should adopt the RBA in order to inform the appropriate level of CDD to be undertaken for existing customers. For example, if a casino considers that any of its existing customers have not been subject to CDD of a standard equivalent to that required by the AML Handbook, it should adopt the RBA and take remedial action in a manner proportionate to the risks and within a reasonable period of time whilst complying with paragraph 8.5.1.

9. RELIANCE AND OUTSOURCING OF AML COMPLIANCE

9.1 Reliance on a third party

9.1.1 (1) gaming establishment may rely on the following third parties ("qualified professionals") to conduct one or more of the elements of CDD on its behalf:

(a) an authorized person or recognized body;

(b) a law firm, notary, or other independent legal business, accounting firm, audit firm or insolvency practitioner or an equivalent person in another jurisdiction;

(c) a Financial Institution; or

(d) other specialized utilities for the provision of outsourced AML/CFT services.

9.1.2 In complying with paragraph 9.1.1(1) above, a gaming establishment may rely on the information previously obtained by a third party which covers one or more elements of CDD and record-keeping.

9.1.3 Where a gaming establishment seeks to rely on a third party in paragraph 9.1.1(1) it may only do so if and to the extent that:

(a) it immediately obtains the necessary CDD and record-keeping information from the third party in paragraph 9.1.1(1);

(b) it takes adequate steps to satisfy itself that certified copies of the documents used to undertake the relevant elements of CDD and record-keeping will be available from the third party on request without delay;

(c) the third party in paragraph 9.1.1(1)(b) to (d) is subject to AML/CFT Regulation, by another competent authority in a country which demonstrates compliance with the FATF Recommendations and it is supervised and monitored for compliance with CDD and record-keeping and any other requisite AML/CFT Regulations;

(d) the third party referred to in paragraph 9.1.1 (1) has not relied on any exception from the requirement to conduct any relevant elements of CDD and record-keeping which the casino seeks to rely on; and

(e) in relation to compliance with paragraph 9.1.1(2), the information is up to date.

9.1.4 If a gaming establishment is not reasonably satisfied that a customer or beneficial owner has been identified and verified by a third party in a manner consistent with this AML Guidance, the gaming establishment must immediately perform the CDD itself with respect to any deficiencies identified.

9.1.5 Notwithstanding the gaming establishment's reliance on a third party in 9.1.1(1), the gaming establishment remains responsible for compliance with, and liable for any failure to meet the CDD and record-keeping requirements in the AML Guidance.

Guidance

1. In complying with paragraph 9.1.1(3)(a), "immediately obtaining the necessary CDD and record-keeping information" means obtaining all relevant CDD and record-keeping information, and not just basic information such as name and address. However, compliance can be achieved by having the information sent in an email or other appropriate means. For the avoidance of doubt, it does not necessarily require a gaming establishment to immediately obtain the underlying certified documents used by the third party to undertake its CDD because under paragraph 9.1.1(3)(b), these need only be available on request without delay.

2. The Commission would expect a gaming establishment, in complying with paragraph 9.1.1(5), to fill any gaps in the CDD and record-keeping process as soon as it becomes aware that a customer or beneficial owner has not been identified and verified by the third party in a manner consistent with this AML Guidance.

3. If a gaming establishment acquires another business, either in whole or in substantial part, the Commission would permit the gaming establishment to rely on the CDD conducted by the business it is acquiring, but would expect the gaming establishment to have done the following:

(a) as part of its due diligence for the acquisition, to have taken a reasonable sample of the prospective customers to assess the quality of the CDD undertaken and records retained; and

(b) to have undertaken CDD and obtain up to date records on all the customers to cover any deficiencies identified in (a) as soon as possible following the acquisition, prioritizing high-risk customers.

4. Where the legislative framework of a jurisdiction (such as secrecy or data protection legislation) prevents a gaming establishment from having access to CDD information upon request without delay as referred to in paragraph 9.1.1(3)(b), the gaming establishment should undertake the relevant CDD itself and should not seek to rely on the relevant third party.

5. If a gaming establishment relies on a third party located in a foreign jurisdiction to conduct one or more elements of CDD on its behalf, the gaming establishment must ensure that the foreign jurisdiction has AML/CFT regulations which are equivalent to the standards in the FATF Recommendations (see paragraph 9.1.1(3)(c)).

9.2 Outsourcing

9.2.1 A gaming establishment which outsources any one or more elements of its CDD or record-keeping obligations to a service provider (including those within its Group) remains responsible for compliance with, and liable for any failure to meet, such obligations.

Guidance

Prior to appointing an outsourced service provider to undertake CDD or record-keeping, a gaming establishment should undertake due diligence to assure itself of the suitability of the outsourced service provider and should ensure that the outsourced service provider's obligations are clearly documented in a binding agreement.

10. MONEY LAUNDERING REPORTING OFFICER (“MLRO”)

10.1 Appointment of a MLRO

10.1.1 Regulation 22 of the AML/PTF Regulations requires every financial business to appoint a MLRO. Where such other individuals are appointed, it is permissible for its procedures to permit employees to make internal reports to these individuals, on behalf of the MLRO. However, the MLRO has ultimate responsibility for all reports made by employees of the financial business and any other individuals appointed must be answerable to the MLRO. Moreover, where the size of

the business permits, the MLRO may carry on other functions within the financial business, provided that they do not conflict with his duties as MLRO.

(1) A gaming establishment must appoint an individual as the MLRO who has an appropriate level of seniority, experience and independence to act in the role, with responsibility for implementation and oversight of its compliance with the AML Guidance. It must do so by completing and filing with the Commission the appropriate form specified by the Paragraph 8 of the **AML/PTF Code**

(2) The MLRO in (1) must be resident in the Turks & Caicos Islands.

10.1.2 The individual appointed as the MLRO of a gaming establishment that comprises as one officer, partner or principal can, with the prior approval of the Commission be the same person as the officer, partner or principal of the gaming establishment.

10.2 Qualities of a MLRO

10.2.1 Gaming establishments must ensure that its MLRO has:

(a) sufficient and up-to-date qualifications and experience to fulfil the role; also, should be exposed to AML/CFT training at least twelve hours or more annually;

(b) a level of seniority and independence within the Relevant third party to enable him to act on his own authority;

(c) sufficient resources including, if necessary, an appropriate number of appropriately trained Employees to assist in the performance of his duties in an effective, objective and independent manner;

(d) timely and unrestricted access to information the gaming establishment has about the financial and business circumstances of a customer or any third party on whose behalf the customer is or has been acting sufficient to enable him to carry out his responsibilities in accordance with paragraph 10.3.1; and

(e) unrestricted access to relevant information about the features of the Transaction which the gaming establishment has entered into or may have contemplated entering into with or for the customer, or a third party on whose behalf a customer is or has been acting.

10.3 Responsibilities of a MLRO

10.3.1 A MLRO must ensure that he or she implement and has oversight of and is responsible for the following matters:

(a) oversee any deputy MLRO or other staff appointed to assist him; and

(b) maintain full and clear records of all disclosures that he has received and all suspicious activity reports he has made.

(c) take great care to manage relationships with all gaming establishments appropriately to avoid tipping off any third parties.

(d) the day-to-day operations for compliance by gaming establishment with its AML/CFT/PF policies, procedures, systems and controls;

(e) acting as the point of contact to receive notifications from the gaming establishment's employees under paragraph 13.2.2;

(f) taking appropriate action under paragraph 13.3.1 following receipt of a notification from an employee;

(g) making reports in accordance with AML Regulations and SARs as prescribed in POCO;

(h) acting as the point of contact within the gaming establishment for the Commission regarding ML/TF/PF issues;

(i) responding promptly to any request for information made by the Commission;

10.4 Money Laundering Compliance Officer

10.4.1 Gaming Establishments must also appoint an MLCO. The MLCO can be the same person as the MLRO and, in the case of a regulated person, can be the same person as the person appointed as Compliance Officer for the purposes of regulatory compliance, if approved by the Commission. However, a regulated person may split the reporting and compliance functions and appoint different individuals as its MLRO and MLCO.

Guidance

1. Gaming establishments are reminded that under Regulation 21 of the AML/PTF Regulations requires every financial business to appoint a MLRO and/ or MLCO function in these mandatory

appointments. For the avoidance of doubt, the individual appointed as the MLRO of a gaming establishment, other than a Representative Office, is the same individual who holds the Recognized Function of MLRO of that gaming establishment. The MLRO is expected to act as a filter and not to routinely pass all disclosures made to him to the Financial Intelligence Agency without making his own assessment.

11. AML/CFT TRAINING AND AWARENESS

11.1 Training and awareness

11.1.1 A gaming establishment must:

(a) provide AML/CFT training to all relevant employees at appropriate and regular intervals;

(b) ensure that its AML/CFT training enables its employees to:

(i) know the identity, and understand the responsibilities, of the gaming establishment's MLRO and his or her deputy;

(ii) understand the relevant legislation relating to AML/CFT/PF.

(iii) understand its policies, procedures, systems and controls related to AML/CFP/PF and any and all subsequent amendments;

(iv) recognize and deal with transactions, risks, trends, techniques and other activities which may be related to money ML/TF/PF;

(v) understand the types of activity that may constitute suspicious activity in the context of the business in which an employee is engaged and that may warrant a notification to the MLRO under paragraph 13.2.2;

(vi) understand its arrangements regarding the making of a notification to the MLRO under paragraph 13.2.2;

(vii) be aware of the prevailing techniques, methods and trends in ML/TF/PF relevant to the gaming establishments;

(viii) understand the roles and responsibilities of employees in AML/CFT/PF, and

(ix) a general understanding of the relevant findings, recommendations, guidance, directives, resolutions, Sanctions, notices which relates to AML/CFT/PF.

(c) ensure that its AML/CFT training:

(i) is appropriately tailored to the gaming establishments' activities, including its products, services, customers, distribution channels, business partners and the level and complexity of its transactions; and

(ii) indicates the different levels of ML/TF risk and vulnerabilities associated with the matters in (c) (i); and

(d) ensure that its AML/CFT training is up-to-date with ML/TF/PF trends, methods and techniques.

11.2 Record-keeping

11.2.1 All relevant details of the AML/CFT training must be recorded, including:

(a) dates when the training was given;

(b) the nature of the training; and

(c) the names of the employees who received the training.

11.2.2 These records must be kept for at least six years from the date on which the training was given.

Guidance

1. The Commission considers it appropriate that all new relevant employees of a gaming establishment be given appropriate AML/CFT/PF training as soon as reasonably practicable after commencing employment with the gaming licensee, and thereafter on a periodic basis.

2. A relevant employee would include a member of the Senior Management or operational staff, any employee with customer contact or which handles or may handle customer monies or assets, and any other employee who might otherwise encounter matters surrounding AML/CFT/PF in the business.

3. Relevant employee should take an RBA to AML/CFT/PF training. The Commission considers that AML/CFT/PF training should be provided by a gaming establishment to each of its relevant employees at intervals appropriate to the role and responsibilities of the employee. The Commission expects that training should be provided to each relevant employee at least annually.

4. The manner in which AML/CFT/PF training is provided by a Relevant employee need not be in a formal classroom setting, rather it may be via an online course or any other similarly appropriate manner.

12. SUSPICIOUS ACTIVITY REPORTS

12.1 Reporting requirements

12.1.1 A gaming establishment must establish and maintain policies, procedures, systems and controls in order to monitor and detect suspicious activity or transactions in relation to potential ML/TF/PF as prescribed in Paragraph 37 of the AML/PTF Code.

12.1.2 A gaming establishment must have policies, procedures, systems and controls to ensure that whenever any employee, acting in the ordinary course of his employment, either:

(a) knows;

(b) suspects; or

(c) has reasonable grounds for knowing or suspecting, that a Person is engaged in or attempting money laundering or terrorist financing, that Employee promptly notifies the gaming establishment's MLRO and provides the MLRO with all relevant details ("Internal Suspicious Activity Report").

12.1.3 A gaming establishment must have policies and procedures to ensure that disciplinary action can be taken against any employee who fails to make such a report.

Guidance

1. Circumstances that might give rise to suspicion or reasonable grounds for suspicion of ML/TF/PF include:

(a) transactions which have no apparent purpose, which make no obvious economic sense, or which are designed or structured to avoid detection;

(b) Transactions or activity which is inconsistent with a patron's normal known activity;

(c) where the size or pattern of transactions, without reasonable explanation, is out of line with any pattern that has previously emerged or may have been deliberately structured to avoid detection;

(d) a customer's refusal to provide the information requested without reasonable explanation;

(e) Frequent cash out transactions without corresponding buy in transactions;

(f) Use of the gaming establishment's account as a savings account;

(g) Suspicious use of counter checks or markers;

(h) Inquiry about end of business day;

(i) not limited to other threats like structuring payments, and other activities that may be deemed suspicious.

2. CDD measures form the basis for recognizing suspicious activity. Sufficient guidance must therefore be given to the gaming establishment's employees to enable them to form a suspicion or to recognize when they have reasonable grounds to suspect that ML/TF/PF is taking place. This should involve training that will enable relevant employees to seek and assess the information that is required for them to judge whether a person is involved in suspicious activity related to ML/TF/PF.

3. The requirement for employees to notify the gaming establishment's MLRO should include situations when no business relationship was developed because the circumstances were suspicious.

4. Effective CDD measures and record-keeping may provide the basis for recognizing unusual and suspicious activity. Where there is a customer relationship, suspicious activity will often be one that is inconsistent with a customer's known legitimate activity, or with the normal business activities for that type of account or customer. Therefore, the key to recognizing "suspicious activity" is knowing enough about the customer and the customer's normal expected activities to recognize when their activity is abnormal.

12.2 Suspension of Transactions and "no tipping-off" requirement

12.2.1 A gaming establishment must not carry out transactions that it knows or suspects or has reasonable grounds for knowing or suspecting to be related to ML/TF/PF. All known or suspected

suspicious transactions must be reported to the FIA. It is an offence to disclose or provide information to anyone that a transaction is deemed to be suspicious and has been reported to the FIA.

Guidance

1. If an employee of a gaming establishment reasonably believes that performing CDD measures will tip-off a customer or potential customer, it may choose not to pursue that process and should file a SAR. Gaming establishments should ensure that their employees are aware of and sensitive to these issues when considering the CDD measures.

3.Pursuant to Section 54 of PTO**,** a person has a duty to disclose information relating to offences and acts of terrorism to the authorities charged with the regulation of such matters. Therefore, the legislation states that a person who has information which will be of assistance in-

(a) preventing the commission or attempted commission by another person, of an act of terrorism; or

(b) securing the arrest or prosecution of another person for an offence under this Ordinance,

shall without delay disclose the information to a police officer.

13. FINANCING OF TERRORISM ("TF") AND WEAPONS OF MASS DESTRUCTION ("PF")

13.1 Financing of Proliferation of Weapons of Mass Destruction

13.1.1 A gaming establishment and/or gaming operator must ensure that their businesses are not utilized in the facilitating of Terrorist Financing, or the financing of the proliferation of weapons of mass destruction (PF). As such, pursuant to the **Prevention of Terrorism Ordinance (PTO) and Counter-Terrorism (Sanctions) (Overseas Territories) Order 2020**, **and Chemical Weapons (Sanctions) (Overseas Territories) Order 2020**, it is an offence for an individual or a financial institution to finance terrorism or the proliferation of weapons of mass destruction.

13.2 Financing of Terrorism

13.2.1 Gaming establishments and Gaming Operators should note that the offence of financing of terrorism is committed where:

Any person who by any means, directly or indirectly, wilfully raises or arranges funds for terrorism, arrange for retention or control of terrorist property provides or collects funds, or attempts to do so, with the intention or in the knowledge that such funds are to be used in whole or in part --

(a) invites another to provide property, receives, provides, or possesses property; and

(b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism;

(c) conducts and or constitutes an offence under or defined in **the Prevention of Terrorism Ordinance.**

13.3 Gaming establishments and Gaming Parlours Reporting Requirements under PTO and POCO

13.3.1 Gaming establishments are required to report to the FIA where the it has knowledge or reasonable grounds to suspect that an activity or a transaction is done for the purpose of the TF or PF. In this regard, **Section 18 (1), (2), & (5) of the PTO** specifically indicates that:

> (**18.1)** Where a financial institution knows or has reasonable grounds to suspect any property in its possession or control, is owned or controlled by an individual or organisation who -
>
> (a) commits acts of terrorism or participates in or facilitates the commission of acts of terrorism or the financing of terrorism; or
>
> (b) is a terrorist organisation,
>
> the financial institution shall report the existence of such property and any information which the financial institution has reasonable grounds to suspect is information regarding a transaction or proposed transaction in respect of such property to the Financial Intelligence Agency.

(**18.2)** Where a financial institution suspects or has reasonable grounds to suspect that property is connected with or related to, or to be used for acts of terrorism or by a terrorist organisation or those who finance terrorism, the financial institution shall report to the Financial Intelligence Agency the particulars related to the persons, accounts and transactions involved, whether complete or not, and the total value of such property.

(**18.5)** A financial institution which fails to comply with subsection (1) and (2) commits an offence and is liable on conviction or indictment to a fine or to imprisonment for a term of seven years, or to both.

13.3.4 Additionally, Section 127 of POCO requires a person to make a disclosure to the Financial Intelligence Agency or to his MLRO if the person:

(a) knows or suspects, or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering; and

(b) the information or other matter on which his knowledge or suspicion, came to him in the course of a relevant business.

(c) the information or other matter must be disclosed as soon as is practicable and, in any event, within **twenty-four hours** after it comes to him.

14. EMPLOYEE SCREENING, TRAINING AND AWARENESS

14.1 Employee Interviews

It is vital that gaming establishments screen their employees in an effort to ensure that employees are of a high standard of integrity. Therefore, gaming establishments are required to vet the competence and probity of employees whose duties relate to the provision of relevant business at the time of their recruitment. The process of employee screening (or vetting) can include:

- Verification of Employee Name(s) and Residential address;
- Confirming the employment history and qualification of the individual;
- Requesting and verifying details of any regulatory action taken against the employee;
- Requesting and verifying the details of any criminal convictions;
- Checking if the individual should be considered a PEP;
- Checking individual against sanctions list;

- Checking the individual's financial solvency.

14.1.2. Employees who are dishonest can pose a fraud and business risk to the gaming establishments.

14.2 Employee Training

14.2.1 Employees who are untrained or alternatively, poorly trained can pose a business risk to gaming establishments. As such, the AML/PTF Regulations require that a financial business must provide all employees whose duties related to the provision of relevant business, with the appropriate training in the recognition and handling of transactions carried out by or on behalf of any person who is, or appears to be, engaged in ML/TF/PF. Thus, all gaming establishments at a minimum shall ensure that relevant employees receive training pertaining to:

(a) the recognition and handling of unusual, complex, or higher risk activity and transactions; such as activity outside of the expected patterns, unusual patterns of business relationships;

(b) ML/TF/PF trends, typologies and any new developments with regards to AML/CTF/PF;

(c) management of customer relationships which have been the subject of SAR, e.g., risk of committing the offence of tipping off, and dealing with questions from such customers, and/or their adviser.

(d) relevant legislations such as the Gaming Control Ordinance, **TCI Regulations, Technical Standards & Internal Controls for Electronic Gaming Devices and Systems**, The Proceeds of Crime Ordinance, the AML/PFT Regulations and the AML/PFT Code and any subsequent amendments; and the relevant guidance issued by the Gaming Control Commission which relates to AML/CFT;

(e) the implications of employees' non-compliance with the AML Guidance issued by the Gaming Control Commission.

14.2.2 Relevant gaming establishments could address the requirement for ongoing employee training through the utilization of training plans or schedules. Essentially, training must be provided to all new employees prior to their being actively involved in day-to-day operations. Thereafter, the training frequency should be in line with a risk-based approach which would enable the gaming establishment to customize the training appropriate to the needs and functions of each employee, and the likelihood of encountering suspicious activities. Nevertheless, employees with responsibility for the handling of customer relationships or transactions should receive more frequent training.

14.2.3 Additionally, employees should be made aware that they have personal responsibilities in the area of reporting. Therefore, training materials should be updated regularly and records must be kept of all training given to employees together with confirmation that they have reached the necessary level of understanding and competence.

14.2.4 Third Party Agreements: A relevant gaming establishment should not enter into an outsourcing agreement with a third party for AML/PTF unless it is satisfied that the third party is suitably qualified and knowledgeable to undertake the outsourced work. In the event that a gaming establishments should engage with a third party to fulfil a function in relation to AML/PTF, it is required to provide appropriate training to the staff of the third parties concerning the specific AML/CFT procedures of the business and potential risks that the business faces.

14.2.5 For the purposes of this section of the AML Guidelines, the term "relevant employee" can include but are not limited to:

- Relevant employees also include any member of the gaming establishment's management or Board of Directors. It follows that the management and Board of Directors should receive comprehensive AML/CTF/PF training in the areas identified above;
- Employees who organise or effect gambling transactions. Therefore, those employees who have direct contact with customers' relationships or financial or gambling transactions.

15. NEW TECHNOLOGIES

15.1 IT Department

15.1.1 The Gaming Industry in the Turks & Caicos Islands is constantly evolving as products and systems are subjected to continual technological advancements. Hence, the Gaming Control Commission is statutorily obligated to ensure that ML/TF/PF risks associated with the use of new or developing technologies for both new and pre-existing products are minimal to non-existent. As such, the Commission requires a gaming establishment or gaming house operator to conduct a risk assessment prior to the launch of new products, business practices or the use of new or developing technologies.

15.1.2 As technology changes, the systems which are managed by this department shall include but not be limited to the systems which are used to monitor, record, and gaming establishments' revenue and that of player tracking data. These systems shall also be able to produce reports so as to enable the gaming establishment and the Commission to evaluate and conduct analysis of patrons gaming behaviours. Therefore, the security and data integrity of these systems are of the utmost importance, particularly where it concerns persons permitted to logically access data particularly at a senior or an administrator level.

15.2 Slot Machines

15.2.1 The Commission's procedures relative to importation, installing, and upgrading of slot machines is to ensure that such devices are not used to facilitate ML/TF/PF.

15.2.2 Prior to a gaming establishment undertaking any system upgrade as it relates to a slot machine, for instance a percentage change, denomination change, or a bill validator upgrade; the gaming establishment shall furnish the Commission with all details surrounding the upgrade. All afore-mentioned upgrades have the capacity to affect player tracking data. Therefore, the gaming establishment shall ensure the integrity of data remains intact and that there is no loss of data as a result of the upgrades.

16. RECORD KEEPING AND RETENTION

16.1 Overview of Record Keeping & Retention

16.1.1 Gaming establishments are required to retain records to ensure that there is readily available information in respect of a full audit trail of the gaming transactions made by its patrons. Whereas, in the event that a financial or other investigation is undertaken by a law enforcement body or by the Commission for compliance purposes, the retention of records will greatly assist in the investigation. Also, it ensures that criminal funds are kept out of the gaming industry, or if not, that they may be detected and confiscated by the appropriate authorities.

16.1.2 Pursuant to section 103 under the Gaming Control Ordinance, a gaming operator shall ensure that all records relating to its gaming operations are kept in a location and a manner as may be prescribed; also kept in a manner which will permit a reconstruction of individual transactions (including the amount and type of currency involved, if any) so as to provide, if necessary, evidence for prosecution of an offence.

16.1.3 Records Retention Standards is the responsibility of each gaming establishment to comply with the AML/PTF Regulations AML/PTF Code, and the obligations imposed on gaming establishments to retain and maintain records pursuant to this AML Guidance. This includes but not limited to all forms, reports, accounting records, ledgers, subsidiary records, computer generated data, internal audit records, correspondence, and personnel records, slot machine analysis report to reflect turnovers and pay-out per gaming device and compare actual hold percentages periods may be specified by the Commission.

16.1.4 Records of identification and verification of customers must be kept for a period of five (5) years after the business relationship with the customer has ended, for example where the customer closes his gambling account with the operator or ceases to visit or use the gaming establishment. All supporting documents relative thereto should also be retained for the relevant five (5) years from the date of the transaction, or date of completion of any related transaction.

16.2 Casinos

16.2.1 As such, pursuant to Section 101 under the Gaming Control Ordinance, every casino operator shall keep, in relation to each patron of the casino to whom the casino operator grants credit, as the case may be -

(a) when a gaming operator opens an account, inclusive but not limited to a copy of signed agreement and any supporting documents, amendment or supplementary agreement thereto for not less than five (5) years after the expiry of the agreement;

(b) when the gaming operator enters into a cash transaction with a patron involving $3,000 or more in a single transaction or when a gaming operator receives a sum of $3,000 or more in a single transaction to be deposited to in patron account; a gaming operator shall ensure to secure these records for not less than five (5) years after the completion of the transaction to which the record relates;

(c) when the gaming operator permits cheque-cashing for the patron, a copy of the signed application, cheque, or any supporting documents shall be secured for not less than five (5) years after the expiry of the facility.

16.3 Slot Parlours

16.3.1 In addition to any other record required by the Proceeds of Crime Ordinance, the AML/PTF Regulations, AML/PTF Code and the Gaming Control Ordinance, , slot parlours shall maintain complete and accurate records of all matters related to interactive gaming activities, including without limitation the following -

(a) the identity of all current and prior registered players;

(b) all information used to register a patron;

(c) a record of any changes made to a patron account;

(d) a record and summary of all person-to-person contact, by telephone or otherwise, with registered player;

(e) all deposits into and withdrawals from a patron account;

(f) a complete game history for every game played including the identification of all registered players who participate in a game, the date and time a game begins and ends, the

outcome of every game, the amounts wagered, and the amounts won or lost by each registered player; and

(g) disputes arising.

16.3.2 A slot parlour shall preserve the records by this regulation for at least five (5) years after they are made. Such records may be stored by electronic means, but must be maintained on the premises of the licence holder or must otherwise be immediately available for inspection.

16.4 General Requirements

16.4.1 As a general summary, the records that gaming establishments must retain are inclusive of but not limited to the following information -

(a) **Transactional Documents**: such as records or transactions carried out by patrons which, as at a minimum, identifies the patron, the nature and the date of the transaction, the type and amount of the currency involved, and the identifying number of any account involved in the transaction.

(b) **Customer Due Diligence Information**: In relation to the evidence of a customer's identity, gaming establishments must keep a copy of any documents or information obtained to satisfy the CDD measures required under the AML/CTF Regulations and Code. As a matter of best practice, any current, additional information or findings relating to the customer, unusual or suspicious transactions (including the background and purpose of any such transactions); should also be retained.

(c) **Training**: Gaming establishments should retain records of any training undertaken in relation to AMML/CFT matters.

Essentially, the Commission expects gaming establishment to use reasonable endeavours to create and keep supporting records and make it clear in their policies, procedures and controls what records will be created in light of the known spending patterns and the assessed ML/TF/PF risks at each premises or locations.

17. CHARITY EVENTS AND TOURNAMENTS

17.1 Charity Events

17.1.1 Pursuant to section 63 of the Gaming Control Ordinance ("GCO"), a charitable gaming or special game of chance licence is required to be obtained from the Managing Director for any scheme that includes the elements of prize, consideration and chance where a person pays something of value to play a game of chance with the opportunity to win a prize.

17.1.2 All charities or organizations may only be issued a licence under this section upon meeting the criteria within the prescribed standards outlined in Section 64 of the GCO.

17.2. Tournaments

17.2.1 A tournament is offered to gaming customers where they can compete against the gaming establishments on games like video slots, blackjack, roulette and poker or against other players for a guaranteed prize.

17.2.2 Pursuant to Section, 166 (h) of the GCO, the Minister may, after consulting with the Commission, make regulations generally giving effect to this Ordinance and specifically in respect of anything required or permitted to be prescribe in the Ordinance; h) provide for tournament play in any gaming facility.

17.3 The AML Risks Posed by Tournaments

17.3.1 Tournaments and Charity Games can pose AML risks to gaming operators. As it relates to casinos, the risk of money laundering activity will increase as casinos being to host high dollar player-to-player tournaments. Further, a central AML issue involving social, skill-based games is the risk of player collusion. Subsequently, gaming establishments should assess their AML policies to mitigate the risk of player collusion in competitive skill-based games.

17.3.2 Accordingly, gaming establishments should also ensure that every patron who uses a skill-based machine or enters a skill-based gaming tournament first presents identification so that the gaming establishments can verify the patron's identity as per KYC requirements.

17.3.3 Further, gaming establishments should consider AML "red flags: for collusion specific to skill-based games that would trigger the need to conduct EDD measures, or even file a STR, on a patron.

17.3.4 Overall, skill-based competitive games have the potential to bring new players and novel AML challenges into the gaming establishments environment. The Commission expects gaming establishments to increase their AML/CFT/PF capacity to mitigate against existing and emerging risks posed by skill-based games, while also complying with all technical standards prescribed under any existing or future Regulations for Gaming Establishments including the Gaming Regulations, Technical Standards & Internal Controls for Electronic Gaming Devices and Systems.

18. SANCTIONS

18.1 Overview

18.1.1 Financial sanctions are provisional measures imposed on individuals or entities in an effort to change undesirable behaviour and curtail their activities, limit opportunities for undesirable and to exert pressure and influence in an effort to prevent and suppress criminal activities in relation to ML/TF/PF.

18.1.2 Gaming establishments and Gaming Operators are precluded from engaging in any form of business with designated persons who are included on the UN or the UK Sanction Lists, and any other Sanctions List from other international organisations that may be stated by the AMLC from time to time. While the purpose for sanctions in the international community is extensive, the ultimate goal of sanctions is to reduce the risk of ML/TF/PF. Therefore, the Commission requires gaming establishments to take steps to access such listings as a part of their EDD process. Accordingly, systems must be put in place to ensure that gaming establishments do not conduct business with designated persons. Furthermore, both residency and nationality shall be

established, or to ensure that appropriate EDD measures are carried out on persons who are from countries listed by FATF as a jurisdiction that is under increased monitoring.

Additionally, licensees can refer to the below list of websites which comprises information relative to Financial Sanctions Notices:

- Turks & Caicos Islands' Attorney General's Chambers- Financial Sanctions Notices – Click Here
- The United Kingdom's Consolidated List –Click here.