GAMING COMMISSION
OF GHANA

# Anti-Money Laundering/Combating the Financing of Terrorism & Proliferation

## GUIDELINES FOR OPERATORS OF GAMES OF CHANCE

2025

ISSUED BY
THE GAMING COMMISSION AND THE
FINANCIAL INTELLIGENCE CENTRE

Table of Contents

## ABBREVIATIONS

AI- Accountable Institution

AML - Anti-Money Laundering

AML/CFT & P -Anti-Money Laundering/Combatting the financing of Terrorism and Proliferation

AMLRO - Anti-Money Laundering Reporting Officer

CDD - Customer Due Diligence

CFT - Combating the Financing of Terrorism

CPF- Combating Proliferation Financing

CTR – Cash Transactions Reporting

DNFBPs - Designated Non-Financial Businesses and Professions

EDD -Enhanced Due Diligence

FATF- The Financial Action Task Force

FIC - Financial Intelligence Centre

GRA - Ghana Revenue Authority

ML/TF - Money Laundering and Terrorist Financing

ML - Money Laundering

MOU -Memorandum of Understanding

ORC – Office of the Registrar of Companies

P -Proliferation

PF- Proliferation Financing

SDD -Simplified Due Diligence

STR – Suspicious Transaction Report

PEPs - Politically Exposed Persons

KYC - Know Your Customer

NRA - National Risk Assessment

TF - Terrorism Financing

## FOREWORD

The gaming industry is experiencing a period of unprecedented growth and transformation. The digital evolution of the internet has brought a significant shift from land-based casinos to online gaming platforms.

The gaming industry, which includes both online platforms and physical structured casinos, is considered a high-risk environment for money laundering due to its large volume of cash transactions, potential for anonymity, and its global presence, which allows criminals to obscure the origins of illicit funds.

Amidst the exciting future of the gaming industry promises, advancement in technology, growing player base, the evolving nature of the gaming landscape and the potential for innovative game experiences, it is important that the industry to adequately prepare to address any identified risks. In the same instance, the industry has become an attractive target for illicit financial activities across the globe.

The need for countries to have in place robust anti-money laundering, combatting the financing of terrorism and proliferation financing mechanisms, coupled with the enhancement of transparent financial systems cannot be over-emphasized. Ghana is determined to maintain a sound financial system and to join global efforts in the fight against this global menace. These efforts can be achieved through dedicated steps to ensure compliance of operators of games of chance through regulations and industry standards that govern both online gaming and physical gambling activities.

In pursuit of the above, the Gaming Commission in collaboration with the Financial Intelligence Centre (FIC) has developed this Anti-Money Laundering /Combatting the Financing of Terrorism and Proliferation Guideline to assist operators of games of chance to design and implement their respective AML/CFT & P compliance frameworks in response to industry best practices and national laws.

This Guideline is issued in reference to the Anti-Money Laundering Act, 2020 (Act 1044), the Gaming Act, 2006 (Act 721) and other relevant laws as well as international best practices. It provides guidance to sector players as to their AML/CFT & P obligations, the need for cooperation, Know Your customer procedures, transaction monitoring, monitoring the conduct of employees, risk assessments, applying risk-based approach, sanctions screening and knowing when to apply enhanced measures on both new and existing clients.

**THE GAMES COMMISSIONER**

**GAMING COMMISSION OF GHANA**

**THE CHIEF EXECUTIVE OFFICER**

**FINANCIAL INTELLIGENCE CENTRE**

## INTRODUCTION

The last two decades have been marked by sophisticated technology and the process of globalization, which has resulted in serious global economic impact. The speed of financial transactions, the dynamism of the gaming industry and its related platforms for moving funds (both legitimate and illicit) across borders have enabled fintech-created opportunities worldwide.

The global gaming market size was valued at USD 249.55 billion in 2022, anticipated to grow from USD 281.77 billion in 2023, estimated to be $522.46 billion in 2025 and projected to reach over $691 billion by 2029. Revenue in the online gambling market is expected to reach $132.9 billion in 2029, up from $97.2 billion in 2024.

Many people worldwide are inclined toward gaming as one of their major sources of entertainment. Online platforms and mobile applications have definitely accelerated the business in the past few years. Despite stringent regulations and heightened due diligence, online gambling remains a lucrative avenue for illicit actors seeking to launder their dirty funds

Illicit financial flows related to cyber-enabled fraud can negatively impact the gaming industry as criminals are always exploiting new ways to hide the illicit proceeds. The Financial Action Task Force (FATF) has identified an increase in the activities of illicit flows in related sectors using virtual assets.

As technology became prevalent, money laundering became easier and attractive in the phase of increased betting terminals. This method requires no human interaction until it comes to cashing out. Know-your-customer (KYC) and CDD processes were not robust thereby guaranteeing anonymity of gamblers within the sector.

Operators of games of chance globally are expected to have mechanism in place to know their customers, verify their identities and continuously monitor all their transactions within the industry. They are also to report any unusual or suspicious financial activities that may indicate potential money laundering, terrorist financing or proliferation of weapons of mass destruction. Gaming companies are to maintain accurate records of identification, verification and transactions to assist competent authorities in their investigations of operators and clients involved in financial crimes.

To mitigate the effect of money laundering, terrorist financing and proliferation risks, regulators, law enforcement agencies and competent authorities are to enhance collaboration with stakeholders, both domestically and internationally.

## BACKGROUND

Ghana conducted its National Risk Assessment (NRA) in 2014 and identified some deficiencies within its AML/CFT &P Framework within the various sectors of the economy. The Gaming sector

was identified as a high-risk sector with the potential to attract criminals to channel their illicit proceeds. Consequently, a number of corrective measures were implemented to ensure that the industry is positioned to fight money laundering, terrorist financing and proliferation financing. These efforts influenced the re-rating of the gaming sector to Medium Risk when the NRA was reviewed in 2018.

Between 2014 and 2018, the Gaming sector supervised by the Gaming Commission had put in place measures to address identified deficiencies which included the setting up of the Anti-Money Laundering Unit within the Commission, training of the staff of the Commission, conducting AML/CFT onsite inspections and organising series of awareness creation programmes for operators of games of chance. These efforts resulted in the gaming sector being re-rated to medium risk of money laundering during the review of the NRA in 2018.

In September 2016, Ghana was subjected to undergo the Second Round of Mutual Evaluation exercise to assess the adequacy and effectiveness of its AML/CFT & P systems in place. One of the outcomes of the exercise was the development of a National Anti-Money Laundering and Combating the financing of Terrorism (AML/CFT &P) policy aimed at addressing the identified deficiencies within the various sectors of the economy. As part of its remedial measures, the Gaming Commission was to issue an AML/CFT & P Guidelines for operators of games of chance or AIs and to put in place measures to enhance compliance among sector players.

Among other requirements by law, the operators of games of chance or AIs are to conduct Know Your Customer/Customer Due Diligence (KYC/CDD), put in place mechanisms to detect, keep records and report suspicious activities of clients, employees and management. Operators of games of chance or AIs are to submit statutory returns to the Gaming Commission and other competent authorities.

Also, the passage of the Anti-Money Laundering Act, 2020 (Act 1044) intensified Ghana's efforts towards the fight against money laundering, terrorism and proliferation financing (ML/TF&PF). Particularly with the powers of supervisory bodies to implement AML/CFT & P measures as part of prudential requirements and to put in place effective mechanisms to enhance the country's AML/CFT & P regime.

This Guideline has incorporated essential elements of the Gaming Act 2006 (Act 721), the Anti-Money Laundering Act, 2020 (Act 1044), Anti-Terrorism Act 2008, (Act 762) as amended and Regulations, relevant Financial Action Task Force (FATF) Recommendations and other international best practices on industry standards and Anti- Money Laundering and the Combating of the Financing of Terrorism and the Proliferation of Weapons of Mass Destruction (AML/CFT&P).

## OBJECTIVE OF THIS GUIDELINE

This AML/CFT &P guideline is intended to guide operators of games of chance or AIs as they establish processes and procedures towards regulatory compliance. It also compliments the legal and regulatory frameworks governing games of chance businesses and their operations.

The objective of this Guideline is to;

(a) encourage the culture of compliance among operators of games of chance.
(b) deter criminals from co-mingling their illicit proceeds through the financial system.
(c) detect and disrupt money laundering activities, ensuring the integrity of the financial system.
(d) encourage operators to report suspicious activity including the predicate offenses to money laundering and terrorist financing and proliferation financing.
(e) enable operators of games of chance to observe and adhere to strict regulatory compliance.

## PART ONE - OBLIGATIONS AND CO-OPERATIONS WITH COMPETENT AUTHORITIES

In line with the Financial Action Task Force (FATF) Recommendation 2, countries are to put in place mechanisms for national AML/CFT/CPF policies, informed by the risks identified, which should be regularly reviewed, and should designate an authority or have a coordination or other mechanism that is responsible for such policies. Countries are to ensure that policy-makers, the financial intelligence unit (FIU), law enforcement authorities, supervisors and other relevant competent authorities, at the policymaking and operational levels, have effective mechanisms in place which enable them to cooperate, and, where appropriate, coordinate and exchange information domestically with each other concerning the development and implementation of policies and activities to combat money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. This should include cooperation and coordination between relevant authorities to ensure the compatibility of AML/CFT/CPF requirements with Data Protection and Privacy rules and other similar provisions.

In accordance with section 37 of Act 1044, the Gaming Commission shall co-operate and share information with any other competent authorities in the performance of its functions. Where a competent authority or any other public agency suspects, in the discharge of responsibilities, information that may be related to money laundering, terrorist financing and proliferation, tax evasion or any other unlawful activity shall report to the Centre within twenty-four hours.

## Powers of the Gaming Commission

Section 3 of the Gaming Act 2006 (Act 721) mandates the Commission to regulate, control, supervise and monitor the activities of the gaming sector. The vision of the Commission is to create a better and sustainable gaming industry for national development and to create and maintain a viable, fair and respectable gaming industry for all who have interest in or are affected by gaming in the country. The Commission shall keep and maintain a register of license which shall contain details of license granted.

## Requirements for a gaming license

Section 13 of Act 721 sets out the basic requirements to operate a game of chance. It provides that a person shall not operate a game of chance if that person is not a limited liability company registered by the Office of the Registrar of Companies and licensed by the Board of the Commission to operate a specified game of chance.

## Conditions for a license

The conditions for the grant of a license are set out in Section 14 of Act 721. It provides that an applicant shall have an identifiable office, registered with the Office of the Office of the Registrar of Companies, meet the minimum capital requirement, have positive feedback on criminal checks, submit financial records, tax clearance certificate, be partly or wholly owned and also demonstrate its readiness to comply with laws and other directives by the Gaming Commission. A license granted under section 43 of Act 721 is also subject to the terms and condition that the Bard may specify in the license.

As part of the licensing requirements, Licensees, its directors, shareholders, and key staff are expected to comply with the following:

- Complete and return Personality Note Form.
- Complete and return AML/CFT &P forms.
- Shall be vetted for a “Fit and Proper” Test.

## Category of License

The categories of games under the purview of the Gaming Commission are as follows:

i) Casinos - A Casino is a facility/business establishment where gambling games are played. This may include the following; blackjack, poker and other gambling tables.
ii) Betting – Betting is an activity whereby sports gamblers predict the outcome of a game by either legally placing a wager on the outcome of a game through a bookmaker or through privately run enterprises.
iii) Route Operations – Is a company that owns and runs slot machines in several locations. Provision of such services allows small businesses to provide slot machines.

iv) Marketing Promotions – Is a strategy used by businesses or licensees to inform or persuade target audiences of the relative merits of a product, service, brand or issue, with the aim of increasing awareness, sales and creating brand loyalty. A society may promote a game of chance if the sale of tickets by the society is confined to members of the society and the society is established and conducted for purposes other than for gaming or betting.
v) Other game of chance permitted by the Commission through the use of tickets, tokens or documents which is evidence of the claim of a person's participation in the game of chance.

## On-site Inspection

Section 26 of Act 721 requires all licensed companies to keep records of its operations as prescribed by the Commission and other related laws. It also empowers officers of the Gaming Commission to inspect these records as and when necessary, during onsite inspections.

Also, section 27 of Act 721 provides that the Board of the Gaming Commission may appoint inspectors to perform its functions. An inspector authorized by the Board may enter premises or a place used or suspected to be used for a game of chance at a reasonable time to investigate activities and make a report to the board. An inspector shall produce an inspector's authorization to the operator of games of chance or AI upon request. The Commission has adequate powers to inspect operators of games of chance for AML/CFT & P infractions and apply appropriate sanctions.

Again competent authorities including police officers not below the rank of Assistant Superintendent may enter the premises if that officer has reasonable cause to believe that an offence with respect to Act 721 is being committed.

## Anti-Money Laundering/Combatting the Financing of Terrorism & Proliferation (AML/CFT & P) Obligations

Section 35 of the Anti-Money Laundering Act, 2020 (Act 1044) provides that the Gaming Commission shall not issue a licence or renew a licence for the operations of game of chance under the Gaming Act, 2006 (Act 721) unless the applicant provides proof of;

(a) the lawful origin of the capital intended for the operation, in the case of the application of a licence; or

(b) the origin of the additional capital, in the case of application for the renewal of licence.

In compliance with sections 52(1) and (5) of Act 1044, the Gaming Commission is designated as a supervisory body to ensure supervision and enforcement of compliance by operators of games of chance or AIs in relation to AML/CFT&P requirements within the gaming industry.

The Gaming Commission shall carry out the following functions:

- adopt a risk-based approach in supervising and monitoring operators of games of chance or AIs;
- monitor and periodically assess the level of ML/TF&PF risk of the operators of games of chance or AIs;
- carry out an examination of the activities of operators of games of chance or AIs based on the risk-assessment conducted by the Gaming Commission.
- request production of, access to, the records, documents, or any other information
- relevant to the supervision and monitoring of operators of games of chance or AIs;
- develop guidelines, directives or notices to ensure compliance among operators of games of chance or AIs;
- provide feedback to operators of games of chance or AIs in line with the provisions of Act 1044;
- approve the appointment of the Anti-Money Laundering Reporting Officers (AMLRO) of operators of games of chance or AIs; and
- undertake any other activity necessary for assisting operators of games of chance or AIs to understand their AML/CFT & P obligations under Act 1044.
- Cooperate and share information with the FIC and other competent authorities.
- Impose administrative sanctions for non-compliance with Act 1044 and Act 721.

## CO-OPERATION WITH COMPETENT AUTHORITIES

The Gaming Act, 2006 (Act 721), relevant legislations and policy frameworks have made provision for coordination and co-operation with competent authorities, law enforcement agencies and supervisory bodies and operators of games of chance to share information on potential risks, suspicious activities, investigations, prosecutions, convictions as well as emerging trends in money laundering, terrorist financing and proliferation.

Accordingly, operators of game of chance or AIs shall comply promptly with all requests made pursuant to the law and regulations by the Gaming Commission, the FIC and any other relevant competent authorities.

An operator's procedures for responding to authorized requests for information on ML/TF&PF shall include:

i. conducting searches through its available databases;

ii. responding promptly to the requesting authority the outcome of the search; and

iii. maintaining confidentiality on such requests.

That notwithstanding, a competent authority shall have access to information to perform its functions of combating ML/TF&P. This shall include the sharing of information with competent authorities, and operators of games of chance.

FATF Recommendation 40 stipulates that competent authorities should put in place mechanisms that allows for rapid, constructive and effective international cooperation in relation to ML/TF & P. The Gaming Commission has a number of measures including the signing of Memorandum of Understanding (MOUs) with international bodies to facilitate the sharing and exchange of information.

## PART TWO – AML /CFT & P INSTITUTIONAL POLICY FRAMEWORK

### Institutional Policy on AML/CFT &P

Operators of games of chance or AIs shall have a written policy framework which is approved by its Board of Directors to enable the institution to monitor the activities of clients and file suspicious activity reports where necessary to competent authorities.

Operators of games of chance or AIs shall be alert to the various patterns of play of games of chance that are suggestive of money laundering, terrorist financing and proliferation financing and communicate such red flags to all staff within the institution.

Operators of games of chance or AIs shall formulate and implement internal rules, procedures and other controls that will deter criminals from using their facilities for ML/TF&PF activities and shall ensure compliance with the relevant laws and regulations. The internal rules shall include:

a) programmes to assess the risk related to money laundering, terrorist financing and proliferation.
b) the formulation of control policy on issues of
    i. timing,
    ii. degree of control,
    iii. areas of control,
    iv. responsibilities, and
    v. follow-up mechanisms,

c) monitoring policy programmes related to suspicious or unusual transactions;
d) enhanced due diligence with respect to clients identified as high risk;
e) training of employees;
f) making employees aware of the procedures under these Guidelines, the Regulations, the Act and other policies adopted by the operator of games of chance or AI;

g) the establishment and maintenance of a manual of compliance procedures related to AML/CFT & P; and
h) other policy directives/notices by the Commission.

Operators of games of chance or AIs are required to take appropriate steps to identify, assess and understand their ML/TF&PF risks in relation to their customers, countries or geographical areas, products and services, transactions or delivery channels in a form of an AML/CFT&P framework to guide the staff in the organization.

In assessing ML/TF&PF risks, operators of games of chance or AIs are required to have the following:
i. develop and implement AML/CFT&P risk assessments framework and obtain Board approval before implementation;
ii. Conduct AML/CFT&P risk assessment and submit the results to the Board for approval;
iii. Consider all the relevant risk factors before determining the level of overall risk and the mitigation measures to be applied;
iv. Keep the assessment up-to-date through a periodic review within a two-year cycle. However, in the event of a significant occurrence, the operator of games of chance or an AI shall review and update its risk assessment framework;
v. review AML/CFT&P framework and identify new areas of potential ML/TF&PF risks and shall provide periodic risk assessment report to the Gaming Commission and the FIC;
vi. design additional procedures and mitigants in their AML/CFT&P operational Guidelines for the newly identified risks;
vii. submit to the Gaming Commission and the Centre not later than 15th January of the following year a report containing the new/additional AML/CFT&P specific risks identified with their commensurable mitigants; and
viii. required to conduct additional risk assessment as and when required by the Gaming Commission.

## Risk-Based Approach

The Financial Action Task Force (FATF) identifies the requirement for a risk-based approach which is premised on the understanding that limited resources should be allocated to identified high risks areas in the scope of risk assessments.

The Gaming Commission adopts a risk-based approach to enforcement which includes compliance with AML/CFT & P requirements. Operators of game of chance or AIs are required to take appropriate steps to identify, assess and understand their ML/TF & P risks in relation to their customers, country of origin or geographical locations, gaming products and/or delivery channels.

## Risk Assessment

Operators of games of chance or AIs are to conduct their respective risks assessments to identify which areas of their businesses pose high risk and apply appropriate measures to mitigate the risk. These assessments would differ from operator to operator depending on the size of customer base, products being offered and the profiles of the gaming businesses.

Operators of games of chance or AIs are required to carry out a business risk assessment to identify the ML/TF & P risks they are exposed to and ensure that policies, controls, and procedures are sufficiently robust to prevent and mitigate the risks. The business risk assessment shall be documented and approved by the Board of Directors of the operators of games of chance or an AI and then forwarded to the Gaming Commission for approval.

In assessing ML/TF & P risks, operators of games of chance or AIs are required to have the following processes in place:

a. document their risk assessments and findings in the form of a framework;
b. Consider all the relevant risk factors before determining what is the level of overall risk and the appropriate level and type of mitigation to be applied;
c. Keep the assessment up-to-date through a periodic review; and
d. Provide periodic risk assessment information to the Gaming Commission, the Centre and other competent authorities.

An effective risk assessment shall be dynamic, allows for regular reviews and the allocation of appropriate resources to mitigate the identified risks. The assessment shall align with the following key objectives:

a) Risk identification- Analysis of risks of an operator of game of chance or AI.
b) Risk mitigation- The application of measures which effectively mitigate the identified risks.
c) Risk monitoring - Ensuring there are sufficient review systems is in place to ensure that risks are identified and updates made to company policies to reflect changes in the risk profile of an operator of games of chance or an AI.
d) Documentation - Having internal controls in the form of policies and procedures to ensure that staff carry out their AML/CFT & P obligations under Act 1044.
e) Risk-review -Evaluating the application of controls and procedures to ensure that policies are fit for purpose.

Operator of games of chance or AIs are to categorize customer as low, medium or high risk by developing a risk scoring model. This risk scoring model shall consider a combination of risk factors such a customer type, gaming product, geographical location, deliver channels, beneficial owners and the outcome of required KYC/CDD processes.

## Risk Assessments on New Products

a. Operator of games of chance or AIs shall review, identify and record areas of potential ML/TF & P risks and submit to the Gaming Commission for approval before they are launched.
b. Operators of games of chance or AIs are required to review their AML/CFT&P frameworks from time to time with a view to determining their adequacy and identify other areas of potential risks when introducing new products.

## Role Of the Board of Directors

The Board of Directors have ultimate responsibility for ensuring the effectiveness of the AML/CFT&P compliance programme. In this regard, the Board's oversight in respect of AML/CFT&P shall align with international best practices. The Board shall ensure that there is documented evidence of its oversight function, for example, in minutes of meetings of the Board (or committees of the Board).

Key responsibilities of the Board include:

i. Approving the appointment of the AMLRO;

ii. Approving AML/CFT&P policy/manual;

iii. Approving the AML/CFT&P compliance programme, training programme, compliance reports, Internal Risk Assessment Framework;

iv. Ensuring the establishment of appropriate mechanisms to periodically review key AML/CFT&P policies and procedures to ensure their continued relevance in line with changes in the operator's products and to address new and emerging ML/TF&PF risks;

v. Ensuring the establishment of an appropriate AML/CFT&P risk management framework with clearly defined lines of authority and responsibility for AML/CFT&P and effective separation of duties;

vi. Ensuring that the Board of Directors receive the requisite training on AML/CFT&P at least once a year;

vii. Ensuring receipt of regular and comprehensive reports on the operator's AML/CFT&P function from the AMLRO for its information and necessary action including but not limited to:

a. remedial action plans if any, to address the results of independent audits (either internal or external); regulatory reports received from the Gaming Commission or the Centre on the assessment of the institution's AML/CFT&P programme;

b. results of compliance testing and self-identified instances of non- compliance with AML/CFT&P requirements;

c. recent developments in AML/CFT&P laws and regulations and their implications if any, to the operator of games of chance or AIs;

d. details of recent significant risk events and potential impact on the operator of games of chance or AI; and

e. statistics of statutory report submitted to the FIC or orders from law enforcement agencies and other competent authorities.

Operators of games of chance or AIs shall submit copies of the approved AML/CFT&P policy and manual to the Gaming Commission and the FIC.

## Role of Senior Management

Senior Management is responsible for the day-to-day implementation, monitoring and management of the AI's AML/CFT&P compliance programme, including ensuring adherence to established AML/CFT&P policies and procedures. Among other things, Senior Management should ensure that policies and procedures:

i. Are risk based, proportional and adequate to mitigate ML/ TF&PF risks of the operator of games of chance or the AI;

ii. Comply with all relevant AML/CFT&P laws, regulations and guidelines; and

iii. Exist for succession planning for the AMLRO function.

Senior Management must review policies and procedures periodically for consistency with the operator of games of chance or AI's business model, gaming products and risk appetite. Attention should be paid to new technologies and operators of games of chance or AIs shall identify and assess the ML/TF&PF risks arising from new products; new business practices, new delivery mechanisms, new technologies and put measures in place to mitigate identified risks.

Risk assessments should take place prior to the launch or use of such products/services, channel, business practices and technologies.

Senior Management shall also ensure that:

i. all significant recommendations made by internal and external auditors and regulators in respect of the AML/CFT&P programme are addressed in a timely manner;

ii. relevant, adequate and timely information regarding AML/CFT&P matters is provided to the Board;

iii. the AMLRO receives appropriate training on an ongoing basis to effectively perform his duties;

iv. there is an ongoing employee training programme (at least twice); and

v. the AMLRO and Internal Audit functions are resourced adequately in terms of personnel, IT systems and budget to implement address AML/CFT&P related issues.

## Role of Anti – Money Laundering Reporting Officer (AMLRO)

1. operator of games of chance or AIs shall appoint an Anti-Money Laundering Reporting Officer (AMLRO) of a key managerial level and of minimum Senior Management grade/status or equivalent. This appointment shall be in accordance with Section 50(1)(b) of the Anti-Money Laundering Act, 2020 (Act 1044) and Regulation 5(1) of L.I. 1987.

2. The AMLRO shall report to the Board or a Sub-Committee of the Board to ensure operational independence.

3. The AMLRO must have sufficient authority, independence and seniority to be able to effectively carry out his duties in accordance with the Act 1044 and this Guideline. The identity of the AMLRO must be treated with the strictest confidence by the management and employees of the operator of games of chance or an AI.

The duties of the AMLRO shall include but not limited to the following:

i. Develop written AML/CFT&P policies and procedures that are kept up to date and approved by the Board;

ii. Have oversight of the AML/CFT&P control activity in all relevant business areas for the purposes of establishing a reasonable risk level consistent across the operator of games of chance or AI;

iii. Keep the AML/CFT&P programme current relative to the institution's identified inherent risks;

iv. Receive and vet suspicious (unusual) transaction/activity reports from staff of operator of games of chance or an AI;

v. Conduct regular risk assessments of the inherent ML/TF&PF risks including timely assessments of new products and new technologies to identify potential ML/TF&PF risks and develop appropriate control mechanisms;

vi. File suspicious transactions reports, submit lists of Politically Exposed Persons, file Cash Transaction Reports and other relevant statutory reports to the Gaming Commission, the FIC and other relevant competent authorities;

vii. Conduct periodic assessments of AML/CFT&P control mechanisms to ensure their continued relevance and effectiveness in addressing ML/TF&PF risks;

viii. Ensure systems, resources, including those required to identify and report suspicious transactions and suspicious attempted transactions, are appropriate in all relevant areas of the operator's business;

ix. Ensure that ongoing training programmes on ML/TF&PF are current and relevant and are carried out for all employees, senior management and the Board;

x. Report pertinent information to the Board and Senior Management regarding the adequacy of the AML/CFT&P framework or any associated issues; and

xi. Serve as both liaison officer with the Gaming Commission and the FIC as well as a point-of-contact for all employees on issues relating to ML/TF&PF.

xii. operator of games of chance or AIs shall ensure that the AMLRO have access to all information that may be of assistance to him/her in consideration of a suspicious or unusual transaction/activity report.

xiii. Operators of games of chance or AIs shall ensure that AMLROs are equipped with the relevant competence, authority, and independence to implement the AML/CFT & P compliance programme.

## INTERNAL CONTROLS, COMPLIANCE AND AUDIT

operator of games of chance or AIs shall establish and maintain internal procedures, policies and controls to prevent ML/TF&PF and to communicate these to their employees. These policies and procedures should cover the CDD, record retention, the detection of unusual and suspicious activities and the reporting of suspicious activities.

The AMLRO and appropriate staff are to have timely access to customer identification data, CDD information, transaction records and other relevant information.

AIs are therefore required to develop programmes against ML/TF&PF to include:

i. The development of internal policies, procedures and controls, including appropriate compliance management arrangement and adequate screening procedures to ensure high standards when hiring employees;

ii. Ongoing employee training programmes for employees.

iii. Adequately resourced and independent audit function to test compliance with the policies, procedures and controls.

operator of games of chance or AIs shall put in place adequate structures that ensure the operational independence of the AMLRO.

## EMPLOYEES SCREENING AND EDUCATION

Operators of games of chance or AIs shall ensure that they have in place appropriate procedures for due diligence when hiring employees. This could include background checks and other vetting processes including verification of information given during the recruitment phase, and confirmation of identities of employees. Employees shall be:

- identified and verified;
- screened for fit and proper; and
- receive appropriate training.

Operators of games of chance or AIs shall consider the ML/TF & P risks posed by the different roles within the operations of a game of chance business. There is the need to conduct background checks on staff prior to onboarding and operators are to continuously monitor the activities of employees and report any suspicious activity to the FIC.

### Employee Training Programmes on AML/CFT & P

An operator of games of chance or an AI shall be consistent with these guidelines and as required by law, train its employees on the requirements of these Guidelines and on its internal policies, procedures and controls as well as on new developments, methods and trends in ML/TF & P. Operators of games of chance or AIs shall design comprehensive employee education and training programs not only to make employees fully aware of their obligations but also to equip them with relevant skills to effectively discharge their AML/CFT& P obligations. The timing, coverage, and content of the employee training program shall be tailored to meet the perceived needs of the operators of games of chance or AIs.

Operators of games of chance or AIs are required to submit their annual AML/CFT& P employee training program for the ensuing year to the Commission and the FIC not later than the 31st of December every financial year.

### Elements of Employee Training

The employee training program is required to be developed under the guidance of the AMLRO in collaboration with the management of an operator of game of chance. The basic elements of an employee training program shall include:

i. AML regulations and offences
ii. The nature of money laundering
iii. Money laundering “red flags” and suspicious transactions, including trade-based money laundering typologies in the gaming industry

iv. Reporting requirements
v. Customer due diligence
vi. A risk-based approach to AML/CFT regime
vii. Record keeping, retention and retrieval policy.
viii. Emerging and new trends within the gaming industry.

Operators of games of chance or AIs shall submit a half-yearly report on their level of compliance to the Gaming Commission, the FIC and other relevant competent authorities.

Operators of games of chance or AIs shall ensure that employees are kept informed of new developments within the industry. These updates shall include:

a. Information on current ML/TF&PF techniques, methods and trends;

b. Clear explanation of all aspects of AML/CFT&P laws and obligations; and

c. Requirements concerning CDD and suspicious transaction/activity reporting.

## TESTING FOR THE ADEQUACY OF THE AML/CFT&P COMPLIANCE FUNCTION

1. operator of games of chance or AIs shall make a policy commitment and subject their AML/CFT&P compliance function to independent testing.

2. It is important that these reviews are performed by auditors (internal or External) who have had appropriate AML/CFT&P training and experience in respect of ML/TF&PF risk and an appropriate level of knowledge of the regulatory requirements and guidelines. It is required that the auditor shall determine the adequacy, completeness and effectiveness of the AML/CFT&P compliance function.

3. Where an operator of games of chance or AIs fails to engage the services of an auditor, the Gaming Commission shall appoint a competent professional to perform those functions and the costs shall be borne by the operator of games of chance or the AI.

4. The report of the independent testing/review of AML/CFT&P compliance function shall be submitted to the Gaming Commission and the Centre not later than January 15 of every financial

year.

5. Any identified weaknesses or inadequacies should be promptly addressed by the operator of games of chance or the AI and subsequently provide an update to the Gaming Commission and the FIC.

## PART THREE- CUSTOMER IDENTIFICATION /CUSTOMER DUE DILIGENCE PROCEDURES

### Customer Identification

It is important to distinguish between identifying the customer and verifying the identification document. Customer identification entails the gathering of information on the prospective customer to enable verification to be done.

Identity as set out in the National Identity Register Act, 2008 (Act 750), its Regulations provides the use of attributes such as name(s), date of birth, residential address including the GPS code and digital address, biometric data and other information of the customer.

Where an international passport is taken as evidence of identity for diplomats, the passport number, date and place/country of issue (as well as expiry date where applicable) shall be recorded by operators of games of chance or AIs.

Operators of games of chance or AIs shall not establish a business relationship until all relevant parties to the relationship have been identified, verified and the nature of the gaming business they intend to conduct established. Once the business relationship is established, any inconsistencies identified in the activity of the client can be thoroughly assessed for potential ML/TF&PF risks.

The Gaming Commission requires operators of games of chance or AIs to effectively manage the profile of their customers through identification and verification of data. CDD is intended to allow the Operators of games of chance or AIs to know who its customer is and to build a customer profile based on which the Operators of games of chance or AIs would be able to assess the customer's activity to identify any unusual behaviour. Identification consist in the collection of a series of personal details on the customer and verification consists in confirming the personal details collected for identification purposes using data, information, and documentation obtained from independent and reliable sources.

CDD consists of four measures:

i. Identification and Verification of the Customer
ii. Identification and Verification of the Beneficial Owner
iii. Obtaining Information on the source of funds/wealth
iv. On-going Monitoring
v. Enhanced due diligence/continuous monitoring

## Duty to obtain identification documents

1. The first requirement of knowing your customer for the purposes of ML/TF&P is for operators of games of chance or AIs to be satisfied that a prospective customer is who he/she is or claims to be.

2. Operators of games of chance or AIs shall not carry out gaming business unless they are certain of the identity of their clients. If the client is acting on behalf of another, the operator of games of chance or AI has the obligation to identify and verify the identity of both the client and the beneficial owner prior to the play of game of chance. The details of the beneficial owner would be confirmed at the point of winnings should the client direct payments to be made to third parties.

## Establishment of identity

1. The customer identification process shall not end at the point of establishing the relationship but continue as far as the business relationship exist. The process of verification, validating and updating identity, and the extent of obtaining additional KYC/CDD information shall be the sole prerogative of the National Identification Authority (NIA) for individuals' resident/working in Ghana.

2. The general principles for establishing the identity of customers and the procedures of obtaining satisfactory identification documents at minimum is set out below:

a. AIs shall obtain sufficient information on the:

i. nature of the gaming business that their customer intends to undertake;

ii. purpose for establishing the gaming business relationship;

iii. source of the funds to be used to undertake the gaming activity; and

iv. details of occupation/employment/business activities of clients.

b. operators of games of chance or AIs shall take reasonable steps to keep the information up to date on clients. Information obtained during any meeting, discussion or other communication with the customer shall be recorded and kept in the customer's file to ensure, as far as practicable, that current customer information is readily accessible to the AMLRO or competent authorities upon requests.

## Identification and Verification of Customers

Operators of games of chance or AIs shall obtain from prospective customers the following identification requirements:

a. full name;
b. date of birth;
c. nationality;
d. identity reference number (i.e. passport number; driver's license)
e. postal address;
f. permanent residential address in Ghana;
g. overseas address;
h. the relationship between the client and the beneficial owner.
i. work permits of foreign nationals working in the country.

Whereas identification consists of the collection of a series of personal details on the customer, verification, on the other hand, requires the confirmation of personal details collected for identification purposes using data, information, and documentation obtained from independent and reliable sources. Operators of games of chance or AIs are therefore required to put in place policies to conduct Customers Due Diligence procedures and establish circumstances where additional information is required. Section 48 of Act 721 provides that a person responsible for a gambling machine shall not permit a child to use the gambling machine or to enter a place where the gambling machine is operated.

When using documentary sources for verification purposes, Operators of games of chance or AIs are to ensure as much as possible that the documents obtained are authenticated.

Each Operators of games of chance or AIs shall maintain identification procedures that

a) require the satisfactory production of evidence of the identity of a person before an operator of games of chance or an AI establishes a business relationship with that person;
b) take into account the suspicion of money laundering where the prospective client of the operators of games of chance or an AI is not physically present during the identification process;
c) ensure the discontinuation of the gaming business relationship where an operator of games of chance or an AI is unable to obtain satisfactory evidence of the prospective client's identity;
d) provide that the identity of a person is established where a third person acts on behalf of that person;
e) Allow the operators of games of chance or AIs to obtain information on the purpose and intended nature of a business relationship;

f) require an operator of games of chance or an AI to conduct ongoing monitoring of the activities of clients to ensure consistency in client risks profiles.
g) ensure that information collected under the client due diligence process is kept up to date by regular reviews of client records.

## Identification and Verification of the Beneficial Owner

Operators of games of chance or AIs shall identify beneficial owners used in gaming activities at the point on onboarding and ensure that same beneficial owners are provided at the point of winnings. Any variation to this should arouse the suspicion of an operator of games of chance or an AI for internal investigations. The results of the investigation should be reported to the FIC on grounds of suspicion of client's engagement in ML/TF & P activities.

## Timing of identification

An acceptable timespan for obtaining satisfactory evidence of identity will be determined by the nature of the business, the geographical location of the parties and whether it is possible to obtain the evidence before commencement. However, any occasion when business is conducted before satisfactory evidence of identity has been obtained must be exceptional and can only be those circumstances justified with regards to the risk appetite of the operator of game of chance or an AI.

2. To this end, an operator of game of chance or AI shall:

i. obtain identification evidence.

ii. where the customer does not supply the required information as stipulated above, operators of games of chance or AIs shall immediately discontinue any activity it is conducting for the customer; and bring to end any understanding reached with the customer; and iii. where the operators of games of chance or AI suspects any unusual or ML/TF&P risks, the operator of games of chance or AI shall file an STR/SAR to Centre.

3. The failure or refusal by an applicant to provide satisfactory identification evidence may lead to a suspicion that the client is engaged in some activities of ML/TF&P. The operator of games of chance or AI shall therefore make an STR/SAR to the FIC based on the information in its possession.

5. Operators of games of chance or AIs shall respond promptly to inquiries made by competent authorities.

### Certification of identification documents

To guard against the dangers of identity fraud and ML/TF&PF risks, operators of game of chance or AIs shall take adequate steps to verify the authenticity of the documents with the issuing or identification authority. In the case of Ghana card verification, operators of games of chance or AIs shall have mechanisms in place to confirm its veracity. Other international systems and mechanisms shall be instituted to assist in the verification of foreign identification documents presented by clients.

### Obtaining Information on the source of funds/Wealth

CDD requires that an operator of games of chance or AI identifies the source of funds and wealth (which includes luxury goods and properties) that a customer uses in gaming activities. This identification and knowledge would enable operators of games of chance or AIs to develop ML/TF & P risk profiles for their clients. Having sufficient information would allow the detection of unusual and subsequent reporting of these activities to relevant competent authorities.

Section 40 of Act 721 also prohibits the use of loans acquired by clients for the purposes of gambling, particularly where the lender knowingly lends money for an unlawful purpose. It further states that, an agreement by which a person lends money to another person and security given in respect of that loan shall not be void because the loan is used or is required to be used for gaming or betting or participating in a lottery or for discharging a debt whether valid or not, incurred through gaming or betting or participating in a lottery.

### Ongoing Monitoring

In carrying out ongoing monitoring of a gaming business relationship, operators of games of chance or AIs shall ensure that documents, data or information are kept up to date. This would require:

1. Questioning of the data and information already in its possession whenever any inconsistencies with the same arise however noticed.
2. Obtain fresh identification documents when the expiry date of the old identification documents held on file is reached.

Licensees should determine on a risk-sensitive basis whether any new information needs to be verified or whether changes are so substantial as to require the carrying out CDD afresh.

## CONDUCTING CUSTOMER DUE DILIGENCE

1. operator of games of chance or AIs shall undertake customer due diligence (CDD) per section 30 of Act 1044 when:

a. gaming business relationships are established;

b. carrying out occasional gaming activity. This may include transactions carried out in a single operation or several operations that appear to be linked.

c. Acquisition of prepaid credit cards;

d. There is a suspicion of ML/TF&PF regardless of any exemptions or any other thresholds referred to in this Guideline;

e. There are doubts about the veracity or adequacy of previously obtained customer identification data;

## CUSTOMER DUE DILIGENCE PROCEDURES (IDENTIFICATION AND VERIFICATION)

1. Operator of games of chance or AIs shall identify their customers and verify the customers' identities using the Ghana Card as the sole identifier for all financial and gaming related transactions. All operator of games of chance or AIs are required to carry out and complete CDD procedures in this Guideline. However, in reasonable circumstances, operator of games of chance or AIs may apply the CDD procedures on a risk-based approach.

2. Operator of games of chance or AIs shall identify a beneficial-owner and take reasonable measures to verify his/her identity using relevant information or data obtained from a reliable source to satisfy themselves that they know who the beneficial owner of a gaming business is.

3. Operator of games of chance or AIs shall in respect of all customers determine whether a customer is acting on behalf of another person. Where the customer or any other third party is acting on behalf of another person through the playing of game of chance, the AI shall take reasonable steps to obtain sufficient identification data and to verify the identity of that other person.

4. Operator of games of chance or AI shall obtain information on the source of funds and intended nature of games to be played by their potential customers.

5. Operator of games of chance or AIs shall conduct ongoing due diligence on the clients which may include scrutinizing the pattern of gaming business undertaken by the customer throughout the course of the AI customer relationship to ensure that the pattern is consistent with the AI's knowledge of the customer, its business and risk profiles, and the source of funds.

6. Operator of games of chance or AIs shall develop or acquire automated monitoring tools to monitor all transactions aimed at detecting suspicious transactions by their customers in real time.

7. Operator of games of chance or AIs shall ensure that documents, data or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records particularly the records in respect of higher-risk clients.

8. operator of games of chance or AIs shall screen all customers (existing and new customers) at onboarding and against domestic and international sanctions lists.

## FAILURE TO COMPLETE CDD

1. An operator of games of chance or an AI who is unable to perform requirements under this Guideline:

i. shall not onboard a client, commence business relationship or perform the gaming business; and

ii. shall submit a Suspicious Activity Report (SAR)/Suspicious Transaction Report (STR) to the FIC within twenty-four hours.

2. Operators of games of chance or AIs that have already commenced the business relationship with clients whose CDD could not be completed shall terminate the business relationship and file a STR/SAR to the FIC within twenty-four hours.

## EXISTING CUSTOMERS

1. Operator of games of chance or AIs shall apply CDD/EDD requirements to existing customers on the basis of materiality and risk and to continue to conduct due diligence on such existing relationships at appropriate times.

2. The appropriate time to conduct CDD/EDD by AIs is when:

i. a transaction of significant value takes place,

ii. customer documentation standards change substantially,

iii. there is a material change in the way that the account is operated, and

iv. the institution becomes aware that it lacks sufficient information about an existing customer.

v. in the absence of the above, AIs shall take appropriate steps to update customer records within two (2) years cycle.

3. The operator of games of chance or AIs shall properly identify the customer in accordance with the criteria above. The customer identification records should be made available to the AMLRO, other appropriate staff and competent authorities as and when necessary.

## NEW BUSINESS FOR EXISTING CUSTOMERS

When an existing customer ends a gaming business relationship or enters into a new gaming business relationship with an operator of games of chance or an AI shall apply a risk-based approach to the conduct of KYC/CDD & EDD procedures. This is particularly important:

a. if there was an existing business relationship with the customer and identification evidence had not previously been obtained;

b. or if there had been no recent contact with the customer within the past twenty-four (24) months; or

c. when a previously dormant gaming account is re-activated.

## LOW RISK CUSTOMERS

Operator of games of chance or AIs shall apply reduced or simplified measures where there are low risks. There are low risks in circumstances where the risk of ML/TF&PF is low, where information on the identity of the customer and the beneficial owner of a customer is publicly available or where adequate checks and controls exist elsewhere in other public institutions. In circumstances of low risk, operator of games of chance or AIs shall apply the simplified or reduced CDD procedures when identifying and verifying the identity of their customers and the beneficial owners.

## HIGH-RISK CATEGORIES OF CUSTOMERS

Operators of games of chance or AIs shall perform enhanced due diligence (EDD) for high-risk categories of customers and gaming business relationships. AIs are to adopt EDD procedures on a risk sensitive basis. In adopting the EDD procedures in determining the risk profile, operator of games of chance or AIs shall have regard to the type of customer, gaming product, location of the customer and delivery channels.

## POLITICALLY EXPOSED PERSONS (PEPs)

PEPs are individuals who are or have been entrusted with prominent public functions both in Ghana or in foreign countries and people or entities associated with them. PEPs include persons who are or have been entrusted with a prominent public function by both domestic and international organizations.

Operator of games of chance or AIs are required to have appropriate risk-management systems and procedures to identify when their customer (or the beneficial owner of a customer) is a PEP and to manage any elevated risks. Gaming business relationships with the family and close associates of a PEP should also be subjected to close monitoring.

3. Operator of games of chance or AIs shall, in addition to performing EDD procedures, put in place appropriate risk management systems to determine whether a potential customer or existing customer or the beneficial owner is a PEP.

4. Operator of games of chance or AIs shall obtain senior management approval before they establish a business relationship with PEP and all other high-risk customers.

5. Where a customer has been accepted or has an ongoing relationship with the operator of games of chance or AI and the customer or beneficial owner is subsequently found to be or becomes a PEP or high-risk, the operator of games of chance or AI shall obtain senior management approval in order to continue the business relationship.

6. Operator of games of chance or AIs shall take reasonable measures to establish the source of wealth, and the sources of funds of customers and beneficial owners identified as PEPs or high-risk and report all anomalies immediately to the FIC and other relevant authorities.

7. operator of games of chance or AIs in gaming business relationships with PEPs or high-risk customers are required to conduct enhanced ongoing monitoring of that relationship.

8. operator of games of chance or AIs shall report to the Centre all transactions conducted by PEPs and their close associates.

### Enhanced Due Diligence and Continuous Monitoring

Where an operator of game of chance or an AI is in a business relationship with a Politically Exposed Person (PEP) or identified high-risk person, they shall conduct enhanced due diligence on the identity, source of funds as well as the activities and also continuously monitor the business relationship.

## PART FOUR - Additional Mitigation Measures

Operators of games of chance or AIs are required to conduct an additional risk assessment as and when required by the Commission and shall be guided by the results of national and sectoral risk assessment to conduct their respective risk assessments.

Operators of games of chance or AIs shall provide timely reports of their AML/CFT & P risk assessment, ML/TF & P risk profile and the effectiveness of risk control and mitigation measures to their respective Boards of Directors. The frequency of reporting shall be determined by their Boards.

Some Operators of games of chance or AIs may allocate additional resources to control certain identified risks. However, the responsibility lies with the Operator of games of chance or AIs to understand these dynamics and to mitigate any identified risks.

In identifying potential risks and threats across the industry, it is the responsibility of each Operator of games of chance or an AIs to examine its products, customers, geographical locations and channels of delivery to identify, understand, assess its AML/CFT &P risks and put in place mitigation measures to address the AML/CFT risks identified. The following categories should be considered:

- Country risk - Some countries pose high inherent risk of money laundering/ terrorist financing risks than others. Ghana is not considered high risk and country-risk is not regarded as a significant risk factor. However, Operators of games of chance or AIs shall be vigilant about customers from high-risk jurisdictions for the purposes of profiling and monitoring purposes.
- Customer risk: specific categories of customers and the resulting business relationships.
- Payment risk: payment methods offered by Operators of games of chance or AIs and the degree to which their specific characteristics are vulnerable to ML/TF & P threats.
- Geographical risk: the risks posed by geographical locations in the country(regions/towns)
- Product risk: products offered and the degree to which their specific characteristics may be attractive for the purpose of money laundering, financing terrorism and proliferation. This may include specific vulnerability relating to gaming machines and self-service betting facilities.
- Employee risk: the risks posed by the employees of Operators of games of chance or AIs. This may include attempts to carry out or collude or manipulate records to facilitate money laundering/terrorist financing and proliferation financing activities.

Each category will pose varying degrees of risk which will vary from one Operators of games of chance or AIs to another. When determining the impact of an identified risk, consideration has been given to factors such as:

  - Facilitation of criminal conduct.
  - Risk of regulatory fines and legal prosecution.
  - Reputational damage to Licensees and/or the industry.
  - Loss of business due to customer rejection.

## NEW TECHNOLOGIES AND NON-FACE-TO-FACE SERVICES

Operators of games of chance or AIs shall have policies in place or take additional mitigation measures as may be needed to prevent the misuse of technological developments in money laundering, terrorist financing and proliferation financing schemes, particularly with the rise of online gaming activities.

Operators of games of chance or AIs shall have policies and procedures in place to address any specific risks associated with remote business relationships or transactions. These policies and procedures shall be applied automatically when establishing customer relationships and conducting ongoing due diligence.

Operators of games of chance or AIs leveraging on Artificial Intelligence, machine learning and data analytic technologies to enhance transaction monitoring, risk assessment, identify patterns and fraud detection shall notify the gaming commission and share the results of such assessments with the Commission and the FIC.

## VIRTUAL CURRENCIES AND BLOCKCHAIN ANALYSIS

Operators of games of chance or AIs using virtual currencies and blockchain analysis shall put mechanisms in place to track the movement of transactions, verify all transactions and associated wallets and report any suspicious activity to the FIC.

## Reliance on Third Parties

Operators of games of chance or AIs shall satisfy themselves that the third party is a regulated and has measures in place to comply with requirements of CDD. Operators of games of chance or AIs who rely on third parties shall immediately obtain the necessary information concerning property which has been laundered, or which constitutes proceeds of or means used to or intended for use in the commission of money laundering, financing of terrorism or any other unlawful act. Such Operators of games of chance or AIs shall satisfy itself that copies of identification data and other relevant documentation relating the CDD requirements will be made available from the third party upon request without delay.

Group Businesses – For Operators of games of chance or AIs that rely on a third party that is part of the same business group, the Commission shall ensure that the following circumstances are met:

i. the group shall apply CDD, record-keeping requirements, and programmes against ML/TF &P in line with and the FATF Recommendations 10 to 12 and 18.
ii. the implementation of those CDD and record-keeping requirements and AML/CFT & P programmes is supervised at a group level by a competent authority; and
iii. any higher country risk is adequately mitigated by the group's AML/CFT & P policies.

## HIGH RISK COUNTRIES/HIGH RISK PERSONS

1. Operators of games of chance or AIs shall give special attention to business relationships and transactions with persons from or in countries which do not or insufficiently apply the FATF recommendations.

2. Operators of games of chance or AIs shall report suspicious activities of clients that have no apparent economic or visible lawful purpose of engaging in gaming activities. The background and purpose of such transactions shall be examined and written findings made available to assist FIC to carry out its duties.

3. Operators of games of chance or AIs that do business with foreign institutions which, do not continue to apply or insufficiently apply the provisions of FATF Recommendations, are required to take measures such as the following:

i. Stringent requirements for identifying customers, including identification of the beneficial owners before gaming business relationships are established.

ii. Enhanced due diligence conducted on clients engaging in suspicious gaming activities.

iii. Enhanced due diligence on Politically Exposed Persons (PEPs)

iv.apply sanctions list screening to identified high-risk customers.

## FOREIGN BRANCHES AND SUBSIDIARIES

1. Operators of games of chance or AIs shall ensure that their foreign branches and subsidiaries or parent observe group AML/CFT&P procedures consistent with the provisions of Act 1044 and these guidelines and to apply them to the extent that the local/host country's laws permit.

2. Operators of games of chance or AIs shall ensure that the above principle is observed with respect to their branches and subsidiaries in countries which do not or insufficiently apply such requirements as contained in these guidelines. Where these minimum AML/CFT&P requirements and those of the host country differ, branches and subsidiaries or parent of operators of games of chance or AIs in the host country are required to apply the higher standard and such must be applied to the extent that the host country's laws permit.

3. Where foreign branches and subsidiaries are unable to observe the appropriate AML/CFT&CPF procedures because they are prohibited by the host country's laws, the foreign branch and the subsidiary shall apply additional measures to mitigate the ML/TF&P risks and shall inform the Gaming Commission and the FIC in writing.

## PART FIVE – BUSINESS RELATIONSHIP, TRANSACTION MONITORING, REPORTING AND RECORDKEEPING

### Business Relationship & Occasional Transactions

Operators of games of chance are to carry out CDD measures with respect to each customer making use of gaming accounts within the premises of operators ;of games of chance.

In the case of an occasional gaming activity, the obligation to carry out CDD will be dependent on the value of the transaction reaching or exceeding the specified threshold in a single transaction or aggregated transactions conducted within a day. Whenever an occasional transaction presents a high risk of ML/TF &P, it is recommended that the Operators of games of chance or AIs identify the source of the funds involved in the gaming activity.

Section 39 of Act 1044 provides that a person shall not conduct two or more transactions separately with one or more than one accountable institution so as to

(a) avoid the duty to report a transaction by an accountable institution; or
(b) breach the duty of an accountable institution to disclose information under this Act.

### SUSPICIOUS TRANSACTION REPORTING

Suspicious transaction may be defined as one which is unusual because of its size, volume, type or pattern or otherwise suggestive of known money laundering methods. It includes a transaction that is inconsistent with a customer's known pattern of play of game of chance or engaging in gaming activities inconsistent with his profile or gaming activities involving huge unknown source of funds that lacks economic rationale.

### Development and Implementation of Institutional Policy

1. Operators of games of chance or AIs shall have a written policy framework that would guide and enable its staff to monitor, recognize and respond appropriately to suspicious transactions. A list of Money Laundering/Terrorist Financing & Proliferation "Red Flags" is provided in the Appendix of these Guidelines.

2. AMLROs shall monitor the activities of clients and report any suspicious transactions/activities to the FIC.

3. Operators of games of chance or AIs shall be alert to the various patterns of play in games of chance that are be suggestive of ML/TF&P and shall disseminate to staff of the gaming business.

4. When a staff of an operator of games of chance or AI detects any "red flag" or suspicion in relation to ML/TF&P, the staff is required to promptly report to the AMLRO. Every action taken shall be recorded.

5. Operators of games of chance or AIs that suspect or has reason to suspect that funds or the proceeds of unlawful activity are related to terrorist financing, shall report to the FIC immediately without delay. All suspicious transactions, including attempted transactions are to be reported regardless of the amount involved.

6. Operators of games of chance or AIs, their directors and employees (permanent and temporary) are prohibited from disclosing the fact that a report is required to be filed or has been submitted to the Centre and any other competent authorities. Tipping off is an offence under Act 1044, therefore any person with knowledge of the Suspicious Report filed with the FIC is prevented from disclosing any information in relation to the report.

### Complex, unusual or large transactions

1. Operators of games of chance or AIs shall pay special attention to all complex and unusual patterns of play of games of chance that have no apparent or visible economic or lawful purpose. Examples of such transactions or patterns of transactions include significant amounts of cash used to play any games of chance or betting on sports, transactions that exceed prescribed thresholds, very high balances on casino accounts where permitted and irregular pattern of play on gaming accounts.

2. Operators of games of chance or AIs are required to examine as far as possible the background and purpose of such transactions and to set forth their findings in writing. They are required to report such findings to the FIC within twenty-four (24) hours upon confirmation of suspicion.

### Cash Transaction Report (CTR)

The Centre shall in consultation with the Gaming Commission determine the appropriate threshold for the operators of games of chance as provided by section 40 of Act 1044. Such Cash transaction reports are to be filed by operators of games of chance or AIs within twenty-four hours after a client reaches the threshold during the play of a game of chance.

Operator of games of chance or AIs shall report to the FIC through a prescribed and a secured platform all cash transactions in any currency and on a specified threshold.

### Transaction monitoring systems

1. Operators of games of chance or AIs shall have appropriate processes in place that allow for the identification of unusual transactions, patterns and activities that are not consistent with the customer's risk profile.

2. Operators of games of chance or AIs shall implement processes to analyse patterns of gaming activities by customers to determine if they are suspicious and are to file reports to the Centre.

3. Transaction monitoring processes or systems may vary in scope (automated and complex systems which integrates customer data with pattern of gaming activities) depending on the size, volumes and frequency of play of a game of chance.

4. Monitoring can be either:

i. In real time, in that transactions and/or activities can be reviewed as they take place or are about to take place within the gaming or betting house; or

ii. After the event through an independent review of the transactions and/or activities that a customer has undertaken.

5. The parameters and thresholds used to generate alerts of unusual transactions/activities shall be customized to be commensurate with an operator of games of chance or AI's ML/TF&PF risk profile and the complexity and extent of its business activities.

Findings, analysis and the proposed modifications shall be documented indicating:

i. The rationale for reviewing the parameters and thresholds;

ii. Details of testing; any assumptions made and the analysis of outcomes; and

iii. The changes made to the parameters and thresholds.

## Identification of Designated Entities and Persons & Freezing of Funds

Operator of games of chance or AIs shall identify and comply with reporting and freezing instructions issued by the Gaming Commission, the FIC and any other competent authority regarding individuals and entities designated by the United Nations Security Resolutions Council and any other relevant international body.

2. Notices issued by the FIC in this regard and the consolidated list shall be duly communicated to operator of games of chance or AIs.

3. In accordance with section 63 of Act 1044, AIs shall have specific obligations to immediately report to the FIC where any of the following apply:

i. A person or entity named on the UN or third-party lists enter the facility of an operator of games of chance or an AI for gaming activities;

ii. The operator of games of chance or the AI has reasonable grounds to believe that the designated person or entity has funds to be channelled through the gaming industry; and

iii. If the designated person or entity attempts to enter into a transaction or continue a gaming business relationship, a suspicious transaction/activity report must be submitted immediately without delay to the FIC.

4. Operator of games of chance or AIs shall not enter into or continue such transaction with the designated person or entity. Funds already deposited into gaming accounts by such individuals or entities are to be held by operator of games of chance or AIs shall remain frozen.

5. It shall be noted that third party lists as set out in section 63 of Act 1044 and Act 762 as amended include an obligation to immediately freeze the funds of the listed entity.

6. In such cases, where the AI identifies funds of a listed person in Ghana, the AI should treat such funds as frozen pursuant to the Act 1044 and Act 762 as amended.

7. Terrorist screening is not a risk-based due diligence measure and must be carried out regardless of the customer's risk profile. Operators of games of chance or AIs shall have processes in place to screen customer details against designated lists of persons and entities and to ensure that the lists being screened against are up to date.

8. Operators of games of chance or AIs policies and procedures shall address:

i. The information sources used by the operators of games of chance or AIs for screening;

ii. The roles and responsibilities of the AI's employees and officers involved in the screening, reviewing and dismissing of alerts, maintaining and updating of the various screening databases and escalating potential matches;

iii. The frequency of review of such policies, procedures and controls;

iv. The frequency of periodic screening;

v. How potential matches from screening are to be resolved by employees of operators of games of chance or AIs, including the process for determining that an apparent match is a positive hit and for dismissing a potential match as a false match; and

vi. The steps to be taken by the AMLRO for escalating potential or positive matches to senior management and reporting suspicious or positive matches to the FIC.

## Books and Records

Operators of games of chance or AIs are required to maintain all necessary records of transactions, both domestic and international, for at least five (5) years following completion of the gaming business/activity. This requirement applies regardless of whether the gaming business relationship is ongoing or has been terminated. Operators of games of chance shall keep books and records

with respect to their customers and transactions and shall ensure that they are available on a timely basis to the FIC and other competent authorities. Section 32 of Act 1044 provides that books and records should include the following;

(a) account details, business correspondence, and copies of documents evidencing the identities of customers and beneficial owners obtained in accordance with this Act;
(b) records of transactions sufficient to reconstruct each individual domestic or international transaction for both account holders and non-account holders;
(c) copies of suspicious transactions reports, cash transaction reports and other relevant reports including any accompanying documentation; and
(d) a written record of findings with respect to the transactions refereed to in subsection (5) of section 30.

## Recordkeeping

Operators of games of chance or AIs are to keep and maintain records on due diligence information, training in relation to AML/CFT& P matters and activities undertaken in relation to AML/CFT& P compliance. Records should be kept on all training given to staff and the confirmation that they have reached the necessary level of understanding.

Section 26 (1) of the Gaming Act 2006 (Act 721) also provides that a licensed company shall keep records of its operations as prescribed by the Commission and any other law and shall make those records available for inspection by an authorized officer of the Commission and any financial intelligence unit established by law.

AIs shall keep books and records with respect to customers and transactions and shall ensure that these records are available on timely basis to the FIC and other competent authorities as set out in section 32 of Act 1044.

## Maintenance of records of transactions

1. Operators of games of chance or AIs are required to maintain all necessary records of transactions, both domestic and international, in accordance with section 32 of Act 1044.

2. Operators of games of chance or AIs shall maintain these records in a manner that upon request by the Gaming Commission, the FIC or any other competent authority can be made readily available.

3. The above requirements apply regardless of whether the account or business relationship is ongoing or has been terminated.

4. Examples of the necessary components of transaction-records include customer's and beneficiary's names, addresses, the nature and date of the transaction, the currency and amount involved, the type and identification number.

5. Operators of games of chance or AIs shall maintain records of the identification data, account files and business correspondence in accordance with section 32 of Act 1044.

6. Operators of games of chance or AIs shall ensure that all customer records and information are made available on a timely basis.

### Access to and Retrieval of Data

Operators of games of chance or AIs shall ensure that there is no secrecy or data protection legislation that would restrict free access to the records on request by competent authorities, under a court order or relevant mutual legal assistance procedures. Where it is found that such restrictions apply, copies of the underlying records of identity shall, wherever possible, be sought and retained.

Section 48 of Act 1044 makes provision for offences in relation to records. A person who opens an anonymous account or an account in fictitious name within the operations of gaming business or fails to maintain or provide access to records as required commits an offence and is liable on summary conviction to a fine of not less than five hundred penalty units and not more than four thousand penalty units or to a term of imprisonment of not less than six months and not more than five years or to both.

There is also a provision for unauthorized access to computer systems or application data which states that a person shall not cause a computer system that belongs to or is under the control of the FIC or an operator of games of chance to perform or fail to perform a function without the consent of the FIC or the Operators of games of chance.

Where identification records are held outside Ghana, it will be the responsibility of the AMLRO to ensure that the records are available and meet the requirements as captured in these Guidelines.

### Statistics and feedback

Operators of games of chance or AIs are to submit statistics on the number Suspicious transaction reports and other statutory reports filed with the FIC, while maintaining confidentiality of its content. They are also to maintain statistics on all requests and other correspondence received from competent authorities in relation to predicate offences of ML/TF & P.

## APPENDICES

APPENDIX A

## DEFINITIONS

### Money Laundering

Section 1 of the Anti-Money Laundering Act, 2020 (Act 1044) provides that a person shall not engage in money laundering. A person commits an offence of money laundering if the person knows or ought to have known that a particular property is or forms part of the proceeds of unlawful activity and the person:

a) converts, conceals, disguises or transfers the property,
b) conceals or disguises the unlawful origin of the property, or
c) acquires, uses or takes possession of the property.

### Terrorist Financing

Terrorist financing is where a person intentionally uses, possesses or receives funds which they know, or suspect will be used for the purposes of terrorism. Terrorists may raise funds through both legitimate and illegitimate means. It must be noted that financial transactions associated with terrorist financing tend to be in a smaller amount than it is in money laundering and when terrorist raise funds from legitimate sources, the detection, and tracking of these funds becomes more difficult.

### Proliferation

Financial Action Task Force (FATF) defines proliferation financing to be an act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. United Nations Security Council (UNSCR) adopted resolutions 1718, 1874, 2087, 2094, 2231, 2270, 2321, 2356, and 2397. In relation to the fighting against proliferation financing, FATF has developed specific requirements to implement these resolutions of UNSCR.

In FATF Recommendation 7, countries are required to implement targeted financial sanctions to comply with UNSCRs relating to the prevention, suppression, and disruption of proliferation of weapons of mass destruction and its financing. Accordingly, countries are required to take preventive measures that are necessary to stop the flows of funds or other assets to proliferators or proliferation and the use of funds or other assets by proliferators or proliferation.

Proliferation of weapons does not only involve the production or development or purchase of these weapons and their means of delivery but also buying or obtaining the materials/goods and the knowledge required for weapons development/production.

In line with Act 1044, an operator of game of chance of AI who knows or reasonably suspects that a property is for financing of proliferation of weapons of mass destruction shall submit a Suspicious Transaction Report to the Centre.

## APPENDIX B: SCOPE OF UNLAWFUL ACTIVITIES/PREDICATE OFFENCE OF MONEY LAUNDERING, TERRORIST FINANCING AND PROLIFERATION FINANCING

AIs shall identify and report to the BOG and the FIC, the proceeds of crime derived from unlawful activities including but not limited to the following:

i. Participation in an organized criminal group and racketeering;

ii. Terrorism, including terrorist financing;

iii. Trafficking in human beings and migrant smuggling;

iv. Sexual exploitation, including sexual exploitation of children;

v. Illicit trafficking in narcotic drugs and psychotropic substances;

vi. Illicit arms trafficking;

vii. Illicit trafficking in stolen and other goods;

viii. Corruption and bribery;

ix. Fraud;

x. Counterfeiting currency;

xi. Counterfeiting and piracy of products;

xii. Environmental crime;

xiii. Murder, grievous bodily injury;

xiv. Kidnapping, illegal restraint and hostage-taking;

xv. Robbery or theft;

xvi. Smuggling;

xvii. Tax Evasion;

xviii. Extortion;

xix. Forgery;

xx. Piracy; and

xxi. Insider trading and market manipulation.

xxii. Cybercrime

## APPENDIX C: SOME RED FLAGS OF MONEY LAUNDERING

i. Unexplained source of funds/wealth
ii. Changing the gambling routine for a certain customer in disproportion with his/her income that was declared beforehand.
iii. Buying gambling chips in, then requesting to exchange them with a cheque from the casino.
iv. Converting illicit cash into chips, playing a minimal amount, and then cashing out the chips can obscure the origin of funds
v. Frequent use of virtual currencies that allow complete anonymity.
vi. Gaming products or services that allow the customer to influence the outcome of the game.
vii. Customers who request to exchange large quantities of low denomination banknotes for those of higher denominations.
viii. Adverse media coverage on customers.
ix. Unusual transaction pattern of play of gaming activities.
x. Gaming activities with unregistered geographical locations.
xi. Reluctance to provide information.
xii. Customer exhibit knowledge of reporting threshold and ask questions that points to avoiding being reported of an unlawful activity.
xiii. Suspicious customer activity
xiv. Gaming activities without any rational economic purpose.
xv. Customers transferring proceeds of winnings to various beneficiaries located in high-risk jurisdictions.
xvi. Cryptocurrency deposits into casino accounts or other gaming accounts.

## SOME RED FLAGS OF TERRORIST FINANCING

i) Gaming transactions are structured below the reporting threshold.
ii) Third-party funding without a clear link or a valid explanation.

iii) Customer avoids disclosing their residential address and the nature of their commercial and economic activity.
iv) Customers share the same address without justifiable grounds.
v) Customers' phone numbers and addresses are frequently changed without justifiable grounds.
vi) Cash deposits are made into gaming accounts in security/political conflict zones or neighboring countries.
vii) Frequent cash deposits through cross-border funds into accounts of persons from high-risk jurisdictions.
viii) Purchasing flight tickets and filing visa applications with the purpose of travelling to political or security conflict zones, regions with security or political instability, regions supporting terrorist organizations or terrorist acts, or travelling to countries adjacent to these zones and regions.
ix) Using crowdfunding websites offering options for making donations in favor of countries where conflicts are taking place.
x) Using social media services and Internet communication services for various purposes that are different from the main declared purpose, mainly for promoting fundraising and contacting persons located in conflict zones.
xi) Publications indicating support for extremist acts.

## SOME RED FLAGS OF PROLIFERATION FINANCING

i. Transactions involving dual-use goods, suspicious transactions, opaque end users, and complex structures.
ii. Dealing with sanctioned countries
iii. Use of shell companies
iv. Transactions involving military goods or chemicals.
v. Customer activity does not match the business profile.
vi. Customer is vague, particularly about end user and end use, provides incomplete information or is resistant to providing additional information when sought.
vii. involvement of individuals, entities, or states in activities supporting the development, acquisition, or spread of weapons of mass destruction (WMDs) and their means of delivery.
viii. Unusual purchases of chemicals that are used in explosives manufacturing with no commercial activity justifying the purchase of such materials.

APPENDIX D:

Examples of high-risk customer categories include but not limited to:

i. Non-resident customers;

ii. Private/Prestige banking customers;

iii. Legal persons or legal arrangements such as trusts, customer account that are personal-assets holding vehicles;

iv. Companies that have nominee-shareholders or shares in bearer form;

v. Politically Exposed Persons (PEPs);

vi. Ministries, Department and Agencies (MDAs);

vii. Metropolitans, Municipals and District Assemblies (MMDAs) and other public institutions;

viii. High Net Worth individuals;

ix. Religious Leaders;

x. Chief Executives and Board Members of private-owned companies/corporations

xi. Cross-border banking and business relationships;

xii. Natural or legal persons who do business in precious metals/minerals, petroleum

xiii. Designated Non-Financial Businesses and Professions;

xiii. And other high risk as may be determined by the National Risk Assessment findings.

Examples of PEPs include but are not limited to;

i. Heads of State or Government;

ii. Ministers of State;

iii. Members of Parliament (both local or foreign);

iv. Politicians (including High ranking political party officials);

v. Ministries, Department and Agencies (MDAs);

vi. Metropolitans, Municipals and District Assemblies (MMDAs) and other public institutions;

vii. High ranking political party officials (National, Regional, District and Constituency Executives etc.);

viii. Legal entity belonging to a PEP;

ix. Senior public officials;

x. Senior Judicial officials;

xi. Senior Security officials appointed by Head of State or Government;

xii. Chief executives and Board Members of state-owned

companies/corporations (both local and foreign);

xiii. Family members or close associates of PEPs; and

xiv. Traditional Rulers.

Appendix VI - Table of Offences and Penalties - Sanctions for Non-Compliance

| S/N | SECTION | OFFENCE | DISCIPLINARY/<br>ADMINISTRATIVE PENALTY |
|---|---|---|---|
| | Section 19 (subsection 2) of Act 721<br>A person who transfers a license granted by the Commission commits an offence.<br>*Anybody who receives a transferred license and uses it to operate a business | • Transfer of license | • Conviction to a fine of not less than Five Hundred penalty units or a term of imprisonment of not less than two years or both.<br>In addition,<br>• Shut down and start the process of acquiring the license<br>• Pay a penalty of USD 5000 for every month that the offender has been in operation. |
| | Section 24 of Act 721<br>A License holder who:<br>a) Persistently fails to maintain any amount of cash or cash equivalent determined by the Commission.<br>b) Fails to give notice of a shortfall in the amount of cash or cash equivalent required. | • Failure to maintain cash/cash equivalent<br>• Failure to give notice of shortfall as above | • Penalty not exceeding the cedi equivalent of USD 20,000 for non-compliance<br>• Revocation of its license whichever the Commission determines to be appropriate.<br>• Penalty of USD 5000 for every month that the Licensee failed to meet or maintain the cash flow. |

| | | | |
|---|---|---|---|
| | c) Fails to take action that the Board requires it to take within the time specified. | | |
| | Section 25 (subsection 2) of Act 721<br><br>Where a Licensee fails:<br><br>a) To inform the Commission of the dishonoured cheque for the payment of a win<br>b) Or to pay the winner the sum due within the time specified in twenty-four (24) hours. | Payment of winnings<br><br>• Issuing of dishonoured Cheques<br>• Failure to pay winnings | • The Commission shall ensure payment of the win by Licensee to the Customer within forty-eight hours.<br><br>**Sports Betting/Route**<br><br>• Pay a penalty of USD 100.00 for every day that a Licensee defaults in paying winnings.<br><br>**Casino**<br><br>Pay a penalty of USD 500.00 for every day that a Licensee defaults in paying winnings.<br>• Impose any other sanctions that the Commission considers appropriate. |

| | | | |
|---|---|---|---|
| | Section 33 (subsection 3) of Act 721<br><br>A person who takes part in, promotes or provides facilities for unlawful gaming commits an offence. | • Participation in unlawful gaming<br><br>• Provision of facility for unlawful gaming | • Conviction to a fine of not more than five hundred penalty units or a term of imprisonment of not more than two years or both.<br><br>In addition,<br>• Seize the machine/close down gaming facility being used illegally<br>• Pay a penalty of USD5,000.00 to the Gaming Commission |
| 6 | Regulation 10 of Anti-Money Laundering Regulations, 2011, LI. 1987 | Failure to put in mechanisms to identify PEPs and other high risk clients. | A minimum of 1,000 penalty units. |
| | | Failure of Licensees to perform enhanced due diligence (EDD) on any of their High Risk Customers. | A minimum of 1,000 penalty units. |
| 7 | Section 32 of Act 2020 (Act 1044). | Failure of Licensees to maintain records of transactions for five (5) years. | A minimum of 1,000 penalty units for every year of default. |
| 8 | Section 38 of Act 2020 (Act 1044). | Failure to report Suspicious Transactions to FIC within 24 hours after arriving at a decision. | A minimum of 1,000 penalty units. |
| 10 | Anti-Money Laundering Regulations 33 of LI 1987. | Failure to put in place management information | A minimum of 500 penalty units. |

| | | | |
|---|---|---|---|
| | | systems to monitor, detect, evaluate and generate STRs. | |
| 11 | Section 49 of Act 2020 (Act 1044). | Failure of Licensees to establish internal policies and procedures to prevent money laundering and financing of terrorism.<br>Failure of the Licensee's Board to ensure an effective implementation of the Licensees AML/CFT Compliance Programme. | A minimum of 2,000 penalty units. |
| 13 | GC/FIC AML/CFT Guidelines | Failure of Licensees to file Cash Transaction Reports (CTR). | A minimum of 1,000 penalty units |
| 14 | Section 50 of Act 2020 (Act 1044) | Failure to develop a regular training program and conduct training for its Board/Management/Employees. | A minimum of 500 penalty units. |
| | | Failure to submit and implement board approved end of year employee training program submitted to the Commission. | |
| 16 | GC/FIC AML/CFT Guidelines. | Failure of Licensees to screen and monitor Employees before and after employment. | A minimum of 500 penalty units. |
| 17 | GC/FIC AML/CFT Guidelines. | Failure to assess areas of additional AML/CFT risks. | A minimum of 500 penalty units. |

| | | | |
|---|---|---|---|
| 19 | Section 40 of Act 749 as amended by Section 19 (2) (e) of AML Amendment Act, Act 874. | Failure to conduct an independent test on AML/CFT Compliance Program. | A minimum of 500 penalty units. |
| 20 | GC/FIC AML/CFT Guidelines. | Failure to obtain Board approval of AML/CFT documents and allocate adequate resources | A minimum of 500 penalty units. |
| 21 | GC/FIC AML/CFT Guidelines | Failure of the AMLRO to submit periodic reports on AML/CFT compliance to the Board. This includes training report, Currency Transaction Report, etc. | A minimum of 500 penalty units. |
| 22 | GC/FIC AML/CFT Guidelines. | Failure to develop and implement risk assessment for New Technologies and Online products, services and delivery channels. | A minimum of 500 penalty units. |
| 23 | For all reports to be submitted to the Commission by Licensees. | Matters on submission of required reports:<br>a. non-submission of reports<br>b. Submission of incomplete or inaccurate reports,<br>c. delayed submission. | A minimum of 500 penalty units. |

| | | | |
|---|---|---|---|
| 24 | GC/FIC AML/CFT Guidelines | Failure to comply with interventions of GRA, FIC and other Competent Authorities. | A minimum of 500 penalty units. |
| 25 | GC/FIC AML/CFT Guidelines | Disclosing information on reports to FIC to third parties. | A minimum of 500 penalty units. |
| 26 | GC/FIC AML/CFT Guidelines. | Failure to put in place and implement policies to protect staff when they report STRs in good faith. | A minimum of 500 penalty units. |
| 27 | GC/FIC AML/CFT Guidelines | Opening of anonymous gaming accounts in a fictitious name for a punter. | A minimum of 500 penalty units. |
| 30 | GC/FIC AML/CFT Guidelines | Failure to obtain Senior Management approval to establish business relationships with PEPs. | A minimum of 500 penalty units. |
| 31 | GC/FIC AML/CFT Guidelines | Failure to obtain information on the beneficial owner of accounts where a customer is an intermediary or authorized representative of another party. | A minimum of 500 penalty units. |
| 32 | GC/FIC AML/CFT Guidelines. | Failure to put in place written policies and procedures on CDD/KYC. | A minimum of 500 penalty units. |

| | | | |
|---|---|---|---|
| 33 | GC/FIC AML/CFT Guidelines. | Failure to ensure Foreign Branches and Subsidiaries comply with AML/CFT provisions. | A minimum of 500 penalty units. |

**Source:** *Gaming Commission/ Financial Intelligence Centre Release, August 2025*

## References


The Gaming Act, 2006 (Act 721)

The Anti-Money Laundering Act, 2020 (Act 1044)

Anti-Terrorism Act, 2008, (Act 762) as amended

The Bank of Ghana/Financial Intelligence Centre AML/CFT & P Guideline for Special Deposit Taking Institutions and Non-Bank Financial Institutions, 2022

FATF Recommendations (Revised) 2012

https://www.fortunebusinessinsights.com/gaming-market

https://strivesponsorship.com/wp-content/uploads/2020/03/Global-Esports-Market-Report-2020.pdf

2020 data from the Entertainment Software Association (ESA)

www.anti-money+laundering+guidelinein+the+gaming+industry&client

https://www.pwc.pl/en/articles/aml-compliance-in-gambling-gaming-and-betting-around-the-globe.html

https://www.symphonyai.com/resources/blog/financial-services/money-laundering-risks-gaming-industry/