AML CODE OF PRACTICE FOR
REMOTE GAMING LICENSE HOLDERS

Version 2.0

AS ISSUED BY THE

TOBIQUE GAMING COMMISSION

This AML Code of Practice was enacted by the Tobique Gaming Commission on April 5, 2024 pursuant to Section 22 of the *TOBIQUE GAMING ACT 2023*.

Contents

INTRODUCTION

This AML Code of Practice (the "**AML Code**"), along with the General Code of Practice for Remote Gaming License Holders (the "**General Code**" and, together with the AML Codes, the "**Codes**"), should be read in conjunction with the TOBIQUE GAMING ACT 2023 (the "**Gaming Act**") and the REGULATIONS CONCERNING ANTI-MONEY LAUNDERING AND COUNTER TERRORISM FINANCING (the "**Regulations**") as enacted by the Tobique Gaming Commission (the "**Commission**") pursuant to Section 22 of the *TOBIQUE GAMING ACT 2023* (the "**Gaming Act**"). Together, these documents and the relevant legislation, form the basis on which the Commission, supported by its authorized Direct Licensees, will administer remote gaming based in Tobique First Nation (the "**Territory**"). The Codes should be construed as 'interpretative guidance' to the Act and the Regulations which underpin them.

Tobique First Nation is committed to ensuring that international standards in regards to Anti-Money Laundering and Countering the Financing of Terrorism and Proliferation, as set out in the Financial Action Task Force (FATF) Recommendations (the "**Standards**"), are adhered to by all holders of a Tobique gaming permit, license, or authorisation, (hereinafter referred to as "**Licensees**") in so far as they apply to interactive gaming conducted in and from the Territory.

The Commission as brought into being by the Gaming Act expects Licensees to apply a risk-based approach to the identification, assessment and management of the ML/TF/PF risks relevant to their business and to the gaming industry in which they operate and in so doing take reasonable and proportionate steps to implement a robust and effective AML/CFT program. The Commission places the onus of this responsibility on the Licensees themselves and as such they will be required to demonstrate the existence and effectiveness of their AML/CFT programs. This proof may include, but is not limited to, a concise customer risk assessment methodology and clearly documented policies and procedures, monitoring, reporting and record-keeping.

As compliance with the Gaming Act and Regulations is a condition of the relevant permit, license or authorisation, so is the acceptance of both the Codes deemed to be a condition of the issuance and continued validity of the permit, license or authorisation (collectively, a "**License**"). The Commission will cancel or otherwise invalidate the License of any Licensee which fails to comply with the obligations and requirements stipulated in the Gaming Act, Regulations, and Codes.

PART 1: APPLICATION AND PURPOSE

1. Purpose

The Regulations implement the relevant international best practice AML/CFT standards as laid down in the Financial Action Task Force Recommendations entitled "International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation". This AML Code supports the Regulations and both this AML Code and the Regulations must be

followed by all Licensees.

This AML Code aims to provide operational guidance to Licensees in the interpretation of the Gaming Act and AML Regulations to ensure that the remote gaming sector in Tobique meets the international industry best practice standards as set out in the FATF Recommendations (the "**Standards**").

Licensees should refer to the Regulations and this AML Code when making decisions in respect of their AML/CFT obligations and seek legal advice where necessary. This AML Code is not intended to be a substitute for legal advice.

2. Application

The Regulations and Codes cover all interactive gaming offered from the Territory regardless of the location of the players and including those transactions and processes that are additionally licensed by another regulatory authority as well as those associated with jurisdictions that have no relevant gambling or AML/CFT regulation. The Commission will use its investigative and disciplinary powers to enforce the Regulations and Codes as covered in the Regulations Part 1 Section 2.1[2]

The Commission, or Direct Licensee on behalf of the Commission, may at any time request that the License Applicant provide additional information and/or documentation in support of their application or to satisfy the Commission that the necessary AML/CFT requirements (as laid out in The Regulations) have been adequately satisfied.

3. Effect

The Commission has the power under the Gaming Act to co-operate with other regulatory and law enforcement agencies as covered in the Regulations Part 1 Sections 3 and 6.[3]

4. Definitions

For the purposes of this AML Code:

"Anti-Money Laundering" (AML) should be read as 'Anti-Money Laundering, Countering the Financing of Terrorism and Counter Proliferation Financing' (AML/CFT/CPF), unless otherwise stated.

[2] Part 1, Section 2(1)
[3] Part 1, Sections 3 and 6 of The Regulations

"Regulations" means the Regulations Concerning Anti-Money Laundering and Counter Terrorism Financing as enacted by the Commission pursuant to Section 22 of the Tobique Gaming Act 2023.

"Commission" means the Tobique Gaming Commission.

"Gaming Act" means the Tobique Gaming Act 2023.

All other capital terms not otherwise defined herein shall have the relevant definition and meaning as set out in the Regulations, Part 1, Section 4.[4]

5. Functions and Powers of The Commission and Direct Licensee

5.1 In addition to such functions, roles and powers set out in the Gaming Act and the Regulations, the Commission shall:

5.1.1 coordinate actions relating to the assessment of money-laundering and financing of terrorism risks in and from the Territory, and to apply resources, aimed at ensuring the risks are mitigated effectively; and

5.1.2 based on that assessment, apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified within its area of control.

5.2 The Commission and Direct Licensee, will apply a risk-based approach to enforcement of Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) requirements as covered in the Regulations Part 1 Section 5[5] and to this end may, at any time, decide to conduct an audit of the Licensee's operation and AML/CFT framework to assess the effectiveness of the Licensee's controls and to ensure that it is conducting its operation in compliance with its own AML/CFT Policies and Procedures and all the rules contained within this AML Code, the Regulations and any other applicable guidance.

6 Inter-Agency Cooperation

The Commission has powers under the Act to cooperate with other regulatory and law enforcement authorities as needed and as described in the Regulations Part 1 Sections 3 & 6.[6]

Licensees should have systems in place that bring to the attention of the Commission all external enquiries, including those from other gambling regulators and law enforcement, into ML/TF suspicions of licensed activities.

[4] Part 1, Section 4 of The Regulations
[5] Part 1, Section 5 of The Regulations
[6] Part 1, Sections 3 & 6 of The Regulations

7 Obligation of Confidentiality

All information received from or about Licensees is confidential and may only be disclosed if required for law enforcement or other legitimate reason defined by The Regulations Part 1 Section 7. [7]

[7] Part 1, Section 7 of The Regulation

PART 2: ASSESSMENT OF MONEY LAUNDERING AND FINANCING OF TERRORISM RISKS BY LICENSEES

8 Understanding the Methods and Risks of ML/TF/PF in the Remote Gaming Sector

8.1 Licensees must understand the risks relevant to the gaming sector, and put in place measures to identify, assess and mitigate these risks. Licensees must be aware of their responsibility and liability in respect of money laundering offences initiated in other jurisdictions by punters/customers registered with themselves and engaged in deposit, gambling, withdrawal or money transfer activities.

8.2 Money laundering involves the introduction or movement of funds from illicit or criminal origins within legitimate financial services or businesses in an attempt to clean or legitimise those funds. Where the Punter/ Customer knowingly attempts to 'clean' or legitimise funds from illegitimate origins ('dirty money') by either, *inter alia,* depositing illicit funds into the game and recording a loss or thereafter cashing out legitimate funds in the form of 'winnings', such Customer commits the crime of money laundering.

8.3 The Licensee has an obligation to ensure that it has implemented robust measures to mitigate against these risks and may be held criminally liable if it can be shown that these measures were insufficient.

8.4 The Licensee has an obligation to recognise and safeguard against money laundering being committed 'knowingly' by the Punter/ Customer which, in the context of the remote gaming sector, is likely to occur most commonly in the below three scenarios:

8.4.1 Disguise - The misrepresentation of illicit funds to the operator as arising from a legitimate source (whether the funds are held on account, played or withdrawn).

8.4.2 Conversion – the conversion of 'dirty money' from illicit sources into 'clean money' the source of which appears legitimate (winnings paid out or balances either held on account or withdrawn)

8.4.3 Disposal – the disposal of illicit funds by way of spending or receiving these illicit funds (e.g. the loss of a deposit or the settlement of debts, known as 'credit betting')

8.5 Money laundering risks for Licensees in the remote gaming/gambling sector are generally deemed to manifest themselves through the possible ownership and control of the Licensed entity by criminals or their associates or the attempted use of that Licensed entity as a conduit for money laundering or terrorist financing.

8.5.1 For the former, it is for this very reason that as part of the licence application process, the identification and verification of the corporate and individual owners and controllers of the License Holder entity is vital to mitigating the risk of money laundering in the gambling industry.

8.5.2 The AML Code is however focused on the latter and seeks to address end customer-centric risks.

8.5.3 In addition, AML/CFT risks must be addressed and mitigated in the vendor selection process and in the supply chain.

8.6 Risks related to the financing of terrorism or proliferation financing facilitated through the remote gambling industry manifest themselves in various methods of peer-to-peer fund transfers involving the purposeful transferring of player funds or chips from one player to another within the same country or cross-border. 'Chip-dumping' in poker is an example of such P2P transfer.

8.7 Red Flags - Licensees should be on alert for warning signs of money laundering such as those indicated below:

8.7.1 High losses which are not consistent with the normal activity of the Customer nor in line with such Customer's player profile or documented financial means.

8.7.2 Spikes in player activity: significant increase in the Customer's play or betting activity which appears not to be consistent with known or profiled activity for that Customer.

8.7.3 Avoidance or delay by the Customer to connect personally with the Licensee.

8.7.4 Provision of false or implausible information or documentation by the Customer in a seeming attempt to conceal or withhold information or documentary evidence required for AML/CFT purposes.

8.7.5 Identification of inconsistent personal information or adverse media related to that Customer's reputation, financial standing or previous convictions.

8.7.6 Customer withdrawals not consistent with usual player activity such as minimal play or spend.

8.7.7 'Loading' of remote gambling accounts by means of the transfer of cash funds deposited in person in live betting shops.

8.7.8 Deposits made from corporate cards or accounts and/or by players with access to corporate funds such as senior financial officers.

8.7.9 Problem gambling behaviour resulting in increased wagering levels and frequencies, where customer may be financing addiction from stolen

funds.

8.7.10 A customer misleads a Licensee as to the source of their deposits, where the source of funds is linked to a criminal activity.

8.7.11 A player transfers criminal funds to another player whether by play or by other means. The Customer will still be deemed guilty of money laundering whether or not that player is colluding with that customer.

8.7.12 A customer engages in very low risk gambling activity or in minimal play in an attempt to recycle illicit funds, or a proportion thereof, through gambling facilities.

9 Preparation of the AML/CTF Program

9.1 In keeping with the tenets of both the internationally recognised FATF standards and The Regulations[8], all Licensees should prepare an Anti-Money Laundering and Counter Terrorist Financing Program ("**AML/CFT Program**") consisting of:

9.1.1 Risk Assessment

9.1.2 Policies, Controls and Procedures designed to manage and mitigate the identified risks.

9.2 Licensees will have to establish the means for demonstrating the effectiveness of their AML/CFT Program and controls. Such means will include properly documented AML/CFT risk assessments, policies and procedures as well as detailed record keeping and the maintenance of statistics. The Commission will consider, *inter alia*, internal and external audits, regulatory returns, desk-based reviews, customer engagements and complaints, inspections and/or other suitable and proportionate measures as the means to establish the effectiveness of Licensees' AML/CFT Program, procedures, systems and controls.

9.3 The Commission expects Licensees to take reasonable and proportionate steps, consistent with a risk-based approach and the terms and conditions of their license agreements, to manage their AML responsibilities. Any examination of reported events alleging money laundering will entail establishing whether the Licensee has acted in a manner consistent with this AML Code and reasonable in the circumstances. This approach puts the responsibility for developing and applying adequate and effective AML procedures on Licensees.

9.4 Licensees must implement The Risk Based Approach to Customer risk management.

9.4.1 The Commission expects a risk-based approach which incorporates

[8] Part 1 Section 7

Licensees carrying out their own identification and assessment of their Customers' AML/CFT risk and putting in place control measures to reduce that risk to the lowest practicable level (considering factors such as time, cost and resources in proportion to the size and scale of the business).

9.4.2 Licensees should have credible policies and procedures in this area and ensure those are reviewed and updated in light of changing and emerging risks, vulnerabilities and learnings.

9.5 The Commission, via the Direct Licensee, will regularly review the AML/CFT programs of Licensees.

9.6 When weaknesses are identified, remedial action, including process change, must be carried out by Licensees as quickly as possible to avoid systemic failure.

9.7 Where a Licensee self identifies issues and implements appropriate and prompt remedial action, this will be taken into account by the Commission when considering any enforcement action.

10 Risk Assessment by Licensee

10.1 The Licensee must conduct a risk assessment to identify and assess the money laundering/ terrorist financing risks to which its business may be subject.[9] In so doing, it must take into account the size and nature of its business.

10.2 In carrying out the risk assessment, the Licensee must take into account all relevant money laundering and financing of terrorism risk factors including factors relating to:

10.2.1 its customers;
10.2.2 the countries or geographic areas in which customers reside or operate;
10.2.3 its products or services;
10.2.4 its payments and transactions;
10.2.5 its operational set up and delivery channels; and,
10.2.6 any third parties that provide services to the business.

10.3 Licensees must ensure that the Risk Assessment is kept under regular review. The Direct Licensee will review these documents as part of the initial license application and subsequent renewals thereof.

11 Policies, Controls and Procedures

11.1 The implementation and maintenance of policies, controls and procedures as part of the

[9] Part 2, section 9(1)

Licensee's obligation to mitigate and effectively manage the risks of money laundering and the financing of terrorism identified during the risk assessment process, must include the following[10]:

11.1.1 Risk management practices;
11.1.2 Internal controls;
11.1.3 Customer Due Diligence measures;
11.1.4 Record keeping; and,
11.1.5 The monitoring and management of compliance with such policies, controls and procedures.

11.2 These policies, controls and procedures must, in addition, make provision for the scrutiny of cases where[11]:

11.1.6 Transactions are complex, unusually large or demonstrate an unusual pattern or have no apparent legal or business purpose or otherwise appear suspicious.

11.1.7 New products, new business practices (including new delivery mechanisms) or new technology are adopted by the Licensee; the related ML/TF risks should be assessed, and measures put in place to mitigate these risks.

11.3 The Direct Licensee will review these documents as part of the initial license application and subsequent renewals and might ask for evidence to demonstrate the controls in action.[12]

12 Reliance on Agents or Third Parties

12.1 The Regulations Part 2 Section 11 define the requirements for relying on third parties or outsourcing any part of the due diligence process. Processes can be outsourced, but responsibility cannot. The Licensee must ensure that it has adequate visibility of processes carried out on its behalf and has satisfied itself that the controls implemented by the third party are fit for purpose.

12.2 Licensees may use third parties to provide the information that they use for due diligence purposes, i.e. they may use third party databases or information services, or make reasonable inferences regarding the identity of a customer from their deposit method etc. Where this is done, the Licensee remains responsible for the outcome of the process, and it remains the case that they cannot 'rely' on third parties to have conducted CDD on their behalf. [13]

[10] Regulations, Part 2, Section 10(1)-(3)
[11] Regulations, Part 2, Section 10(4)
[12] Regulations, Part 2, Section 10(4)
[13] Part 2, Section 11(1)-(2)

13 Compliance Officer and Governance Requirements

13.1 Licensees should ensure that the AML/CFT roles and responsibilities of the Board and their senior managers are clearly defined and documented.

13.2 Licensees must appoint a member of senior management to take ownership of the responsibility for implementing, managing and overseeing all requisite AML/CFT measures and thereby ensure compliance with the tenets contained within this AML Code. This senior manager will ensure that the Board and other senior managers are keep appraised of any material ML/TF risks and sign off on/ approve higher risk scenarios where appropriate and will own Board Level accountability.

13.3 In carrying out this function, the nominated Senior Manager may appoint a Senior Compliance Officer or Money Laundering Reporting Officer who will take ownership of the day-to-day management of the Licensee's ML/TF risks. In smaller firms, the Nominated Senior Manager may fulfill the function of MLRO.

13.4 The Senior Compliance Officer or Money Laundering Reporting Officer must have sufficient AML/CFT expertise, experience and knowledge in order to effectively discharge his/ her obligations inherent in the role/function. The Licensee should ensure that the appointed Senior Compliance Officer/ MLRO is imbued with the following:

13.4.1 Sufficient AML/CFT knowledge of the international regulations/ guidance and other applicable AML/CFT legal and regulatory frameworks, and experience in the implementation of AML/CFT controls within similar firms and the gambling industry in particular.

13.4.2 Autonomy in his/ her role to be able to exercise independent influence and provide effective challenge as appropriate.

13.4.3 Sufficient knowledge and understanding of the specific ML/TF risks associated with the gaming/ gambling sector in general and with the remote gaming world in particular.

13.5 The existence of the MLRO and dedicated staff does not exonerate other senior executives from personal or corporate liability for allowing money laundering to occur.

13.6 Escalation of Risks to Board or Risk Committee:

13.6.1 Licensees must have clear and accountable governance processes to review Customer accounts which raise AML concerns.

13.6.2 Material ML/TF risks should be escalated to a senior risk management forum and Licensees must implement governance processes to allow for the escalation of

these risks to either the Board of Directors overseeing the licensed entity, or an appropriate Risk Committee comprised of senior managers and the MLRO.

13.6.3 Such forum must be properly constituted, and minutes of meetings kept, using formal reports and assessment tools for identified cases.

13.6.4 Any such committee may be combined with, or separate from, any similar group established to examine customers raising responsible gambling concerns.

13.7 Annual AML/CFT Reports:

13.7.1 The Board should receive at least an annual report on AML/CFT activities and issues affecting the company from the Compliance Officer, including an annual update of the corporate Risk Assessment and a report on the work of the Risk Management Committee. More regular reports to the Board should be made as events dictate.

13.7.2 The Commission, via the Direct Licensee, may wish to review Risk Assessments and annual board reports.

14 Training

14.1 Licensees must ensure that all staff receive adequate AML/CFT training in order that they might understand the risks and their own responsibilities as regards the prevention and mitigation of ML/TF risks. The training provided may include both general and role-specific training.

14.2 Assessment - After the training each attendee must undergo an assessment to test their recently acquired AML/ CFT knowledge. If a score of at least 75% is not achieved, attendees will be required to re-sit the test and/or repeat the training.

14.3 Annual refresher training - Every year on the anniversary of their initial training and assessment all staff must attend refresher training. Any changes to relevant regulations, policies or procedures should be covered within the scope of this annual training.

14.4 Training must be provided on a regular basis and training records must be maintained in support thereof.

14.5 AML/CFT training should *inter alia* cover the following areas:

14.5.1 Risks of money laundering and terrorist financing relevant to the business, the applicable legislation and staff obligations and responsibilities under the legislation.

14.5.2 The Licensee's Risk Assessment methodology and mitigating policies, controls and procedures.

14.5.3 The identification of potentially suspicious transactions or activity.

14.5.4 Red flags or indicators of money laundering or suspicious activity appropriate to the remote gaming/ gambling sector.

14.6 The Direct Licensee, on behalf of the Commission, will review the records of this training as part of the granting/renewal of a license.[14]

15 Employee Due Diligence

15.1 The Licensee must implement measures for conducting Due Diligence on employees and mechanisms for the ongoing monitoring, management and reporting of control breaches by its employees.[15]

15.1.1 A Licensee must put in place appropriate risk-based systems and controls to determine whether to, and in what manner to, screen any prospective employee who, if employed, may be in a position to facilitate the commission of any money laundering or financing of terrorism offence.

15.1.2 The systems should also describe whether to, and in what manner to, re-screen an employee where the employee is transferred or promoted and may be in a position to facilitate the commission of any money laundering or financing of terrorism offence.

15.1.3 The Licensee must establish and maintain a system for the firm to manage any employee who fails, without reasonable excuse, to comply with any system, control or procedure.[16]

15.2 The Direct Licensee, on behalf of the Commission, will review these arrangements as part of the granting/renewal of licenses.[17]

16 Independent Review

16.1 The Licensee's AML/CFT Program must be subject to regular, independent and, where appropriate, external review.

[14] Part 2, Section 14(1)-(2)
[15] Regulations, Part 2, Section 15
[16] Part 2, Section 15(1)-(3)
[17] Part 2, Section 16(1)

16.2 The frequency of the review should take into account the nature, size and complexity of a Licensee's business, and the type and level of money laundering or financing of terrorism risk it might face but must be undertaken every two years as a minimum. [18]

16.3 The purpose of the review is to:

16.3.1 Assess the effectiveness of the program having regard to the money laundering or financing of terrorism risk of the Licensee;

16.3.2 Assess whether the program has been effectively implemented; and

16.3.3 Assess whether the Licensee has complied with its program.

16.4 The Commission, or Direct Licensee on behalf of the Commission, has the power to require a review to be conducted by an external party if there are concerns about the quality of controls or the reviews conducted.[19]

17 Directions by the Commission and Direct Licensee

17.1 The Commission or the Direct Licensee, acting with the Commission's approval, may issue a direction to a Licensee to adopt additional measures to handle its risks of money laundering and terrorist financing more effectively.

17.2 Without limiting the scope of its power of direction, the Commission or a Direct Licensee may, in the public interest, direct a Licensee:

17.2.1 not to enter into a business relationship with a specified person or class of persons;

17.2.2 not to undertake transactions of a specified description with a specified person or class of persons;

17.2.3 to terminate an existing business relationship with a specified person or class of persons; or

17.2.4 to cease any operations in a particular jurisdiction.

[18] Part 2, Section 16(2)
[19] Part 2, Section 16(1)-(5)

PART 3: CUSTOMER DUE DILIGENCE

18 When to Apply Customer Due Diligence

18.1 In accordance with Recommendation 10 of the FATF Standards, Customer Due Diligence measures should be employed at the following times:

18.1.1 When establishing business relations.

18.1.2 When carrying out occasional transactions.

18.1.3 Where there is a suspicion of money laundering or terrorist financing.

18.1.4 Where there is doubt about the veracity or adequacy of previously obtained customer identification data.

18.2 In keeping with the requirements of the Regulations and within the context of the gaming industry, Customer Due Diligence measures should be commenced at account opening and must furthermore be completed within 30 days of first deposit or before the Customer wagers more than an equivalent of EUR 2,000 of their own funds (as opposed to recycled winnings) and before any money is paid out.[20]

19 Customer Due Diligence

19.1 The identification and verification of the customer, is required in order to:

19.1.1 Understand the potential ML/TF risks associated with the Customer in the context of the business relationship; and

19.1.2 Take appropriate steps to mitigate the risks.

19.2 Customer Due Diligence measures should be employed in accordance with and commensurate to the ML/TF risk found to be associated with that Customer, after taking into account all relevant risk factors (as detailed in section 10(2) above). More onerous Customer Due Diligence measures should be employed in those circumstances where the Customer is deemed to present a higher risk of money laundering or terrorist financing – these are addressed in paragraph 20 below under Enhanced Due Diligence.

[20] Part 3, Section 19

20 Initial Customer Due Diligence:

20.1 Initial Customer Due Diligence refers to the customer due diligence measures which are employed at the start of the Customer Due Diligence or Know Your Client (KYC) process and is comprised of the following checks:

20.1.1 Identification via the registration process and then verification of the Customer's identity using reliable independent or primary source documents (such as government-issued photo ID documents) or other appropriate electronic ID&V software.

20.1.2 Gathering of supporting information and accompanying proofs (such as date of birth and residential address).

20.1.3 Standard screening checks.

20.2 An integral part of the Initial Customer Due Diligence process is the performance of Customer screening. Licensees' customers must be screened against industry standard databases to identify Politically Exposed Persons (PEP), sanctions and adverse media.

20.2.1 Adverse media, PEP and sanctions screening should be initiated at account registration and concluded no later than the point of verification.

20.2.2 Sanctioned customers must not be allowed to deposit and play; sanctions screening must be carried out at the point of registration. Any players infringing international sanctions legislation must be immediately barred from further play.

20.2.3 Accounts with PEP hits are to be frozen pending EDD checks and PEP risk assessment.

20.2.4 Adverse media identified in relation to the Customer must be put through a risk assessment and where applicable, mitigation process.

20.3 Screening 'hits' that are deemed to be relevant and material must be run through a risk mitigation process. High risk factors that are identified during the screening process, may require the employment of Enhanced Due Diligence measures in order to mitigate the risk identified.

21 Enhanced Due Diligence

21.1 Licensees should perform more rigorous Customer Due Diligence checks on higher risk Customers in an effort to mitigate any ML/TF risk associated with those customers. Enhanced Due Diligence checks must be performed on Customers that have been risk rated as High or have associated Red Flags or High-Risk Factors.

21.2 Enhanced Due Diligence measures must go further than the measures applied under Initial or Standard Customer Due Diligence and may include the following:

21.2.1 Obtaining additional information to verify the customer's identity. Certification of identity documents may also be required.

21.2.2 Obtaining additional information as to the customer's source of funds and/or source of wealth.

21.2.3 Enhanced screening – for example using a second search engine in addition to a third-party data provider (e.g. Google screening).

21.2.4 Senior management and MLRO approval may be required for the establishment or continuation of the customer relationship.

21.2.5 Conducting enhanced monitoring of the customer relationship.

21.3 A Licensee must employ Enhanced Due Diligence measures in the following circumstances:

21.3.1 Where there is a change in the risk assessment for that Customer;

21.3.2 Where there is any suspicion regarding the true identity of the Customer;

21.3.3 Where there are any transactions which are not reasonably consistent with the usual activity of the Customer;

21.3.4 Where there is a suspicion of money laundering or terrorist financing; and,

21.3.5 Where there are any doubts about the veracity or adequacy of previously obtained Customer identification data.[21]

21.4 The presence of High-Risk Factors or Red Flags may necessitate the implementation of Enhanced Due Diligence measures and may include:

21.4.1 High Risk Countries or Jurisdictions;

21.4.2 Customer using faked or stolen identification documents;

21.4.3 A Customer excluded for problem gambling reasons who has bypassed blocking measures to start playing again;

21.4.4 Use of high-risk payment methods such as prepaid cards or crypto currency;

[21] AML Regulations, Part 3, Section 20(2)

21.4.5 Significant/Material Adverse Media related to financial crime/ serious or criminal offences/ reputationally damaging news events;

21.4.6 Identification of a Politically Exposed Person (PEP);

21.4.7 Indirect link to a sanctioned individual, entity or country; and,

21.4.8 Customer transactional activity of either high value or high volume may also be deemed to be a high-risk factor especially where it exceeds the customer's estimate affordability levels.

22 Commercial or Business-to-Business (B2B) Relationships

Initial Customer Due Diligence

22.1 Business-to-Business (B2B) License Holders must employ Initial Customer Due Diligence measures on their B2C Operator Customers as part of their onboarding procedures.

22.2 Initial Customer Due Diligence in this context of onboarding of B2C Operator Customers refers to the process of information gathering to identify and verify the Licensee entity, its owners, controllers and other related parties to better identify, assess and manage relevant associated risk factors. This process entails the following[22]:

22.2.1 Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information to understand the ultimate beneficial ownership and control of their B2B customers.

22.2.2 Where the customer is a corporation or other business entity, the License Holder must take reasonable measures to verify the identity of the individual or individuals who are the ultimate beneficial owners of the customer, such that the License Holder is satisfied that it knows who the ultimate beneficial owner is. This may require License Holders to understand the ownership and control structure of the customer.

22.2.3 Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship; and

22.2.4 Understanding the predicted transactional profile of the B2C Operator Customer and where appropriate, the source of funds.

22.3 B2B License Holders who provide customer-facing type services to and on behalf of their B2C Operator Customers, including but not limited to customer services, VIP account

[22] Part 3, Section 19(1)

management, fraud and risk services, must obtain the approval of the Commission or the Direct Licensee on behalf of the Commission and undergo ongoing monitoring by the B2C Licensee to ensure that the services they provide on their behalf meet the requirements and standards necessary to mitigate money laundering and terrorism financing as contemplated in the Codes.

22.4 B2C License Holders accepting business from corporate account holders (including 'hedging accounts', professional betting companies, etc.) must conduct appropriate levels of corporate due diligence on these corporate account holders to determine natural persons who have sufficient equity to qualify for Ultimate Beneficial Owner (UBO) status, upon which the equivalent of Standard/ Initial Customer Due Diligence must be conducted.

22.5 Other relevant B2B Suppliers:

22.5.1 B2B Aggregator License Holders who distribute third party gambling software to B2C Operator Customers must employ Initial Customer Due Diligence measures on their gambling software providers as part of their onboarding procedures.

22.5.2 B2B License Holders who are suppliers of casino table games, or providers of peer-to-peer poker networks or betting exchange platforms have access to real time game play or game performance statistics, betting patterns, wagering levels and collusion activity and therefore will need to ensure that gameplay and betting transactions are monitored in real time for recognised money laundering or terrorist financing 'gameplay' methodologies and reported to their B2C Operator Customer in a timely and proportionate way should they occur, allowing for possible interventions in funds transfers or withdrawals.

22.5.3 Given the evolving nature of ML/TF methodologies, it is expected that the details of the monitoring which will be carried out will be agreed between the parties from time to time and need not be set out in precise detail at the outset. While some methodologies are transparent and easy to identify (e.g. repeated low risk bets in roulette), P2P transfers and chip dumping can be highly sophisticated, shielded and complex.

Enhanced Customer Due Diligence (EDD)

22.6 More onerous Customer Due Diligence measures must be employed where License Holders are deemed to carry a higher money laundering and terrorist financing risk. Enhanced Due Diligence measures are employed in these higher risk circumstances to better understand the customer ownership and control structure and risks specific to the size and nature of the business and customer base. A holistic approach to risk assessment should be employed, the risks considered together and mitigated where appropriate.

22.7 Enhanced Due Diligence measures for corporate entities include, but are not limited to, the following:

22.7.1 Deeper ownership checks for Ultimate Beneficial Owners of the corporate entity (checks down to 10% ownership in the Customer entity are recommended).

22.7.2 Additional Verification of Identity checks – government issued photo-ID documents as proof of identity required for more Directors under EDD measures. Certification of these identity documents may also be required.

22.7.3 Evidence of Source of Wealth and Source of Funds for UBOs.

22.7.4 Enhanced screening – for example using a second search engine in addition to a third-party data provider (e.g. Google screening)

22.7.5 Senior management and MLRO approval may be required for the continuation of the business relationship.

23 Country Risk

23.1 Sanctioned jurisdictions - Tobique will not do business with any entity or individual who is subject to EU, UN, UK, US or other international sanctions legislation. Applicants with related parties on the FATF blacklist will not be eligible for consideration for a Tobique Remote gaming license. This is outside of risk appetite.

23.2 Banned jurisdictions – Any countries that have been placed on the Tobique 'banned list' will be deemed to be out of risk appetite and it will not be permissible for players to exercise their gaming rights under a Tobique remote gaming license from any of these countries.

23.3 High Risk Countries - Where Applicant Licensees or any of their related parties are found to be associated with a High Risk Third Country or any other high-risk jurisdiction on the FATF 'grey' list, Enhanced Due Diligence measures must be employed, and the risks considered holistically in an attempt to mitigate this red flag.

23.4 Please see Appendix A for a list of countries demarcated as being either Banned, High Risk, Medium Risk or Low Risk jurisdictions. This risk factor will be included in the Customer Risk Assessment Methodology and is a significant contributor to the final Customer risk rating.

24 Politically Exposed Persons (PEPs)

24.1 A PEP is "a natural person who is or who has been entrusted with a prominent public function." The precise definition is contained in the Regulation.[23]The Regulations Part 3 Section 21 defines the requirements for detecting and mitigating the risks associated with

[23] Part 3, Section 21(2)

Politically Exposed Persons (PEPs).

24.2 Those individuals who meet the definition of a PEP pose a higher money laundering risk as their prominent political position makes them vulnerable to corruption.

24.3 PEPs must be subjected to Enhanced Due Diligence checks and ongoing monitoring. PEPs must be risk assessed and, if deemed to be material, such PEPs will be subject to enhanced screening and enhanced ongoing monitoring checks. The Licensee's board of directors will need to sign off any PEP play.

24.4 Licensees should note that PEP status itself is intended to apply higher vigilance to certain individuals and put those individuals that are customers or beneficial owners into a higher risk category. It is not intended to suggest that such individuals are involved in suspicious activity.

24.5 For at least 12 months after a PEP is no longer entrusted with a prominent public function, Licensees should consider the continuing risk posed by that person and apply appropriate measures until such time as that person is deemed to no longer pose a further risk specific to PEPs.

24.6 Due to the influence held by individuals holding prominent political positions, 'Politically Exposed Persons' (PEPs) are deemed to represent an extremely high risk from a money laundering perspective. This risk will be further exacerbated when the individual is a direct PEP and linked to either a higher risk jurisdiction or countries with known higher levels of corruption and political/ financial instability. Additional more stringent customer due diligence checks will need to be performed on Customers with PEP associations, a risk mitigation statement produced and approval from senior management required for continuing the business or customer relationship.[24]

25 Ongoing Monitoring

25.1 Licensees and Customers must be subject to ongoing monitoring checks for the duration of the relationship and not just at initial onboarding stage.

25.2 Ongoing monitoring includes but is not limited to the following activities:

25.2.1 Regular screening against PEP, sanctions, and adverse media databases.

25.2.2 Transaction Monitoring activities in terms of which the frequency, volume and value of bets placed by an individual Customer must be monitored and compared to expected customer transactional profiles. Unusual activity will be investigated and, in the case of potentially suspicious activity, will be escalated to the MLRO in the form of a Suspicious Activity Report.

[24] Part 3, Section 21(1) and (3)

25.3 All Licensees and their identified related parties will be subject to ongoing monitoring requirements. License Holders are furthermore expected to subject their Customers in B2C relationships to the same ongoing monitoring measures.

25.4 Ongoing Monitoring checks for Licensees should include the identification and monitoring of 'linked' accounts owned by the same player. It is common practice for players to maintain segregated accounts for different gambling spend but ownership of these accounts must be known and linked and activity across all accounts assessed and monitored together.

26 Periodic Review

26.1 Licensees will be subject to regular reviews, performed periodically, of their Customer Due Diligence and Risk Assessments. The frequency of these Periodic Reviews will be commensurate to the ML/TF risk associated with these entities and their related parties.

26.2 Licensees will be expected to perform similar periodic reviews of the CDD of their Customers/ Punters in B2C relationships aligned to the risk profile of each Customer.

26.3 Periodic Reviews will comprise of a full refresh of all Customer risk assessments, Know Your Customer information and documentation gathered in support of their CDD requirements, Screening against PEP, sanctions and adverse media databases and transaction monitoring reviews to reset Customer transactional profiles.

27 Event Driven Reviews

27.1 An Event Driven Review is comprised of a full refresh of Customer KYC and CDD information and documentation together with a re-assessment of the risk associated with the Licensee.

27.2 The identification of a high-risk factor or red flag during the screening or transaction monitoring processes will trigger an EDR and may include the identification of the placement of unusually large or frequent bets or bets placed during particular times or events.

27.3 A material change to the ownership or control of a License Holder's corporate customer, will trigger an Event Driven Review (EDR).

PART 4: RECORD-KEEPING AND REPORTING

28 Record-Keeping

28.1 License Holders must keep all records obtained through customer due diligence including copies or records of official identification documents, account files and business correspondence, for at least five years after the business relationship is ended, or after the date of the occasional transaction.

28.2 License Holders must maintain records of the originator/payer information, and required beneficiary/payee information, on wire transfers, electronic fund transfers and other electronic payments.

28.3 License Holders must provide the Commission, or Direct Licensee on behalf of the Commission, with a copy of all records as specified by the Commission, whenever a License Holder/ Licensee relocates the business or ceases business.[25]

29 Reporting

29.1 Licensees or License Holders have an obligation to report to the Commission, or Direct Licensee on behalf of the Commission, on any identified instances of suspicious activity where the License Holder knows of or reasonably suspects that certain behaviour on the part of the Customer may be related to money laundering activity or where such activity appears to be unusual or at variance with the usual behaviour or transactional activity of the Customer. License Holders must share all Suspicious Activity Reports with the Commission.

29.2 License Holders may be required to report on request, to the Commission, or Direct Licensee on behalf of the Commission, on additional AML/CFT requirements as deemed appropriate.

[25] AML Regulations, Part 4, Section 4

30 APPENDIX A

RESTRICTED COUNTRY LIST

Country	Country Rating	Region	EU High Risk 3rd Country	FATF Grey List	FATF Black List	UK HR 3rd Country	OECD (Uncooperative tax haven)	CPI	Comprehensive sanctions?	OFAC	EU	UN	HMT
Afghanistan	High Risk	Asia	Yes	No	No	No	No	20	Yes	Yes	Yes	Yes	Yes
Central African Republic	High Risk	Africa	No	No	No	No	No	24	Yes	Yes	Yes	Yes	Yes
China	High Risk	Far East	No	No	No	No	No	42	Yes	Yes	Yes	No	No
Cuba	High Risk	Caribbean	No	No	No	No	No	42	Yes	Yes	No	No	No
Democratic Republic of the Congo	High Risk	Africa	Yes	Yes	No	Yes	No	22	Yes	Yes	Yes	Yes	Yes
Haiti	High Risk	Central America	Yes	Yes	No	Yes	No	17	Yes	No	Yes	Yes	Yes
Iran	High Risk	Middle East	Yes	No	Yes	Yes	No	24	Yes	Yes	Yes	Yes	Yes
Iraq	High Risk	Middle East	No	No	No	No	No	23	Yes	Yes	Yes	Yes	Yes
Israel	Medium Risk	Middle East	No	No	No	No	No	62	No	No	No	No	No
Korea, North	High Risk	Far East	Yes	No	Yes	Yes	No	17	Yes	Yes	Yes	Yes	Yes
Libya	High Risk	Africa	No	No	No	No	No	18	Yes	Yes	Yes	Yes	Yes
Myanmar (Burma)	High Risk	Far East	Yes	No	Yes	Yes	No	20	Yes	Yes	Yes	No	Yes
Russia	High Risk	Russia & CIS	No	No	No	No	No	26	Yes	Yes	Yes	No	Yes
Somalia	High Risk	Africa	No	No	No	No	No	11	Yes	Yes	Yes	Yes	Yes
South Sudan	High Risk	Africa	Yes	Yes	No	Yes	No	13	Yes	No	Yes	Yes	Yes
Syrian Arab Republic	High Risk	Middle East	Yes	Yes	No	Yes	No	13	Yes	Yes	Yes	No	Yes
United Kingdom	Low Risk	Europe	No	No	No	No	No	71	No	No	No	No	No
United States	Low Risk	North America	No	No	No	No	No	69	Yes	No	Yes	No	No
Venezuela	High Risk	South America	No	No	No	No	No	13	Yes	Yes	Yes	No	Yes
Yemen	High Risk	Middle East	Yes	Yes	No	Yes	No	16	Yes	Yes	Yes	Yes	Yes
Canadian Provinces	Low Risk	North America	No	No	No	No	No	76	No	No	No	No	No
Ontario													
New Brunswick													