

AML/CFT/CFP Policy

Aquarius Entertainment N.V.

Curaçao

May 2026



- This anti money laundering counter financing of terrorism and counter financing of proliferation of weapons policy (AML/CFT/CFP Policy) shall apply to all branches and subsidiaries of **Aquarius Entertainment N.V.** (Company).
- This AML/CFT/CFP Policy consists of the main file, which established general principles for certain procedures in the course of the Company's activity and annexes, which describe certain processes and/or requirements in details.
- Implementation of this AML/CFT/CFP Policy will not detract from the obligation to comply with any other local law and is not to be regarded as enabling the implementation of acts that have been prohibited or restricted by local laws.
- The Company maintains full cooperation with law and regulatory authorities in legislations, investigations, and inquiries in Curaçao and abroad.
- The AML/CFT/CFP Policy is accepted and approved by the resolution of the Company's Compliance Officer and managing director.

Administrative information

Company name: Aquarius Entertainment N.V.

Registration number: 161153;

Address: Schottegatweg Oost 10, Bon Bini Business
Center Unit 1-9, Willemstad, Curaçao;

Email: Info@aquariusnv.com

Glossary

AML	Anti-Money Laundering	PEP	Politically Exposed Person
BRA	Business Risk Assessment	RBA	RBA Risk-Based Approach
CDD	Customer Due Diligence	SDD	Simplified Due Diligence
CFT	Counter Financing of Terrorism	SoF	Source of Funds
CFATF	Caribbean Financial Action Task Force	SoW	Source of Wealth
CFP	Counter Financing of Proliferation of Weapons	UN	The United Nations
CRA	Customer Risk Assessment		
EU	The European Union		
EDD	Enhanced Due Diligence		
FATF	Financial Action Task Force		
FIU	Financial Investigation Unit Curaçao		
FT	Financing of Terrorism		
FP	Financing of Proliferation of Weapons		
GCB	Curaçao Gaming Control Board		
ML	Money Laundering		

Table of Contents

GLOSSARY	3
TABLE OF CONTENTS.....	4
INTRODUCTION	8
COMPANY'S KEY AML/CFT/CFP PRINCIPLES	8
COMPANY'S AML/CFT/CFP POLICY	8
REVIEW OF THE AML/CFT/CFP POLICY.....	9
GOVERNANCE PRINCIPLES	10
VIOLATIONS OF THE AML/CFT/CFP POLICY	10
Reporting of Violations.....	11
COMPANY'S SERVICES.....	11
MONEY LAUNDERING	12
FINANCING OF TERRORISM.....	12
FINANCING OF PROLIFERATION OF WEAPONS.....	13
AML/CFT/CFP SYSTEMS.....	13
PRIMARY LEGISLATION GOVERNING AML/CFT/CFP IN CURAÇAO	13
SUPERVISORY AUTHORITIES	15
EFFECTIVE CONTROLS.....	15
THREE LINES OF DEFENSE	16

SENIOR MANAGEMENT RESPONSIBILITIES.....	17
KYC AGENTS.....	17
COMPLIANCE DEPARTMENT	18
Compliance Officer.....	18
Investigation Unit.....	19
AUDIT FUNCTION.....	20
RISK BASED APPROACH (RBA)	20
BUSINESS RISK ASSESSMENT	21
Risk Management Process	22
CUSTOMER RISK ASSESSMENT	23
Determination of the customer's risk profile	24
Maintaining of the customer's risk profile	25
High Risk.....	26
Medium Risk	26
Low Risk.....	26
NON-ACCEPTABLE CUSTOMERS	26
Anonymous accounts.....	27
Prohibited countries.....	27
Inability to complete CDD	27
RISK FACTORS SPECIFIC TO THE GAMBLING SECTOR	27
Customer risk.....	28

Geographical risk	28
Product, service and transaction risk	29
Distribution channels risk	30
TECHNOLOGICAL DEVELOPMENTS RISK ASSESSMENT	30
CUSTOMER ACCEPTANCE POLICY	31
CUSTOMER DUE DILIGENCE	31
Timing of CDD Measures and Minimum Requirements	33
Identification and verification of the customer	34
Identification and verification of the Beneficial Owner	36
Obtaining information on the Purpose and Intended Nature of the Business Relationship	36
Politically Exposed Persons identification	37
Reliance on Third Parties and Outsourcing	38
SIMPLIFIED DUE DILIGENCE	39
ENHANCED DUE DILIGENCE	40
Politically Exposed Persons	41
Source of Wealth and Funds	42
ONGOING DUE DILIGENCE	44
Ongoing monitoring of identity	44
Ongoing monitoring of transactions	44
<i>Risk-based approach to monitoring</i>	45
<i>Methods and procedures</i>	45

REFUSAL OR TERMINATION OF THE BUSINESS RELATIONSHIP	47
TARGETED FINANCIAL SANCTIONS	48
PROCEDURE FOR IDENTIFYING THE SUBJECT OF SANCTIONS AND A TRANSACTION VIOLATING SANCTIONS.....	48
ACTIONS WHEN IDENTIFYING THE SANCTIONS SUBJECT OR A TRANSACTION VIOLATING SANCTIONS	49
REPORTING OBLIGATIONS.....	49
RECOGNITION OF UNUSUAL TRANSACTIONS.....	49
Objective indicators	50
Subjective indicators	50
REPORTING OF UNUSUAL TRANSACTIONS	51
TIPPING OFF.....	52
RECORD KEEPING	53
TRAINING AND SCREENING OF EMPLOYEES	54
INDEPENDENT AUDIT OF THE AML/CFT/CFP POLICY	56
EXAMINATION BY THE GAMING CONTROL BOARD.....	57
ANNEXES	59
VERSION CONTROL TABLE	61

Introduction

The Company adopts appropriate, sufficient measures aimed to preventing its operations from being used as means to conceal, manage, invest or use any form of money – or other assets – due to illicit activities, or to give the appearance of legality to such activities.

The Company adopts a risk-based approach in the design and implementation of this AML/CFT/CFP policy with a view to managing and mitigating ML/FT/FP risks. A qualified Compliance Officer has been appointed to implement appropriate AML/CFT/CFP policies and procedures.

Company's key AML/CFT/CFP Principles

In the course of its business activity, the Company implements the following principles:

- to comply with AML/CFT/CFP legislation in the countries in which it operates;
- to strive to fulfil international standards as detailed by the Financial Action Task Force (FATF) recommendations;
- to work in conjunction with FIU and the governments of the countries the Company operates in, as well as support their objectives in relation to the prevention, detection and control of ML/FT/FP;
- the Company may decide not to provide products or services based upon decisions guided by ML/FT/FP risk appetite and corporate social responsibility;
- to comply with primary legislation of Curaçao on AML/CFT/CFP.

Company's AML/CFT/CFP Policy

The Company has established this AML/CFT/CFP Policy to ensure that any ML/FT/FP risks identified by the Company are appropriately managed and mitigated. This means having adequate systems and controls in place to mitigate the risk of the Company being used to facilitate any financial crimes. This AML/CFT/CFP Policy is designed to represent the basic standards of AML and CFT procedures and standards, which will be strictly observed by Company.

The AML/CFT/CFP Policy is based upon applicable AML/CFT/CFP laws, regulations and regulatory guidance from the Government Institutions of Curaçao. This AML/CFT/CFP Policy is further designed to comply with the Financial Action Task Force (FATF) Standards on combating money laundering and the financing of terrorism and proliferation.

Among other things, this AML/CFT/CFP Policy:

- forms part of its wider compliance regime, and is designed to meet the requirements of its legislative environment;
- ensures that the Company is able to detect suspicious activities associated with money laundering, fraud, and terrorist financing, and report them to the appropriate authorities;
- focuses not only on the effectiveness of internal systems and controls developed to detect money laundering, but on the risk posed by the activities of customers with which Company does business;
- is built on a strong foundation of regulatory understanding and overseen by personnel who are experienced and knowledgeable enough to create a climate of compliance at every level of their organization.

Review of the AML/CFT/CFP Policy

The AML/CFT/CFP Policy is subject to a review by the senior management or the board of directors at least annually. The proposal for a review and the review of these Guidelines may be scheduled more often by the decision of the compliance officer or the Internal Control Officer. The Company must review and, where necessary, update this AML/CFT/CFP Policy and its annexes (incl. the risk assessment policy and risk assessment made thereof) in the each of the following cases:

- publication of the results of the National Money Laundering and Terrorist Financing Risk Assessment;
- upon receipt of an order from the FIU to strengthen the applicable internal procedures;
- upon significant events or changes in the Company's management and operations;
- such necessity arises during periodic monitoring of the implementation and adequacy of the Company's internal policies.

This AML/CFT/CFP Policy's review (incl. regular annual review) shall be confirmed with the relevant resolution signed by the by the senior management or the board of directors.

Governance Principles

The Company's employees and the service providers (third parties) involved in the Company's business should act in accordance with this AML/CFT/CFP Policy. The obligations of the Company as defined in this AML/CFT/CFP Policy must be understood as the duties of all employees of the Company unless it is provided that certain duties must be performed by a specially designated employee of the Company (e. g. the senior management, the Compliance Officer, etc.).

All employees of the Company, depending on the functions performed by them, shall be introduced to this AML/CFT/CFP Policy. They should be aware of their subordination to other structural units of the Company. If the Company has more than 1 employee in a structural unit, the senior management shall appoint a responsible employee whose task is, among other things, to perform daily supervision over the performance of the tasks of the structural unit (or part of it). The Company's senior management must ensure that all newly recruited employees are made aware of this AML/CFT/CFP Policy and the Company's structure. Each employee shall confirm the awareness of and compliance with the AML/CFT/CFP Policy in writing. The Company shall maintain appropriate records of such acknowledgements and may require periodic reconfirmation (incl. as part of ongoing training process).

The day-to-day management of the Company takes place through the senior management. The senior management is responsible for assigning tasks to the Company's structural units and controlling the performance of tasks assigned. In case when the relevant employee or third party is not appointed for performing of structural unit's functions, the senior management shall be responsible for this structural unit's functions. In addition to day-to-day management, the senior management organizes meetings and, if necessary, discusses decision-making with experts (incl. employees, advisors and external service providers).

Violations of the AML/CFT/CFP Policy

Failure to comply with the requirements set out in this AML/CFT/CFP Policy may expose the Company and individuals to significant regulatory, legal, financial, and reputational risks. Violations of this AML/CFT/CFP Policy may result in, among others, the following consequences:

- regulatory investigations, sanctions, penalties, or restrictions imposed by competent authorities;
- civil or criminal liability for the Company and/or the relevant individuals;

- suspension, revocation, or refusal of licenses;
- contractual breaches and termination of business relationships resulting in disruption of business operations;
- financial losses, including penalties, remediation expenses and loss of revenue;
- reputational damage and adverse impact on the Company's market position.

Any breach of this AML/CFT/CFP Policy, whether through intentional misconduct, negligence, failure to report suspicious activity, circumvention of controls, or failure to complete required compliance procedures, may result in disciplinary action. The severity of disciplinary action shall depend on the nature, scope and circumstances of the breach. Disciplinary measures may include:

- formal warning;
- mandatory retraining;
- restriction or removal of access to relevant systems or responsibilities;
- suspension of duties;
- termination of employment or contractual relationship; and/or
- referral to competent regulatory, law enforcement, or other authorities where required by law.

Reporting of Violations

All employees are required to report any actual, suspected, or attempted violation of this AML/CFT/CFP Policy to the Compliance Officer without delay via email or other secure channel. Failure to report known or suspected violations may itself constitute a violation of this AML/CFT/CFP Policy.

Company's Services

The Company is operating as an online casino as it is specified in Curaçao legislation. The Company provides services to a customer allowing for the wagering of a stake with monetary value in a game of chance. In doing so the Company opens an account for their customers. This is considered to be indicative of a relationship that is expected to have an element of duration and is therefore considered a business relationship between the Company and the customer. The Company provides the services only via electronic channels.

Before any changes in way of the services provision, the Company shall assess risks related to such changes.

Money Laundering

All acts done with money of illegal origin to change its identity so that it appears to have originated from a legitimate source, can be considered money laundering (ML). It is the process of making dirty money look clean. Money Laundering consists of three phases:

- Placement. During this stage, the money launderer introduces the illegal proceeds into the financial system through financial institutions, casinos, shops and other cash intensive businesses. This is done among other things by buying chips for cash, then redeeming value without playing or with minimal playing, funding casino accounts with credit and debit cards, prepaid cards, checks and cryptocurrency and then requests for pay out and inserting funds into gaming machines and immediately claiming those funds as credits;
- Layering. This stage involves converting the proceeds of crime into another form to disguise the audit trail, source and ownership of funds. It can involve transactions such as transfers of funds from one account to another, sometimes to or from other casinos or jurisdictions, currency exchange, structuring and refining and gambling accounts held for storing moneys and hiding them from the authorities;
- Integration. The re-entry of funds into the economy in what appears to be normal business or personal transactions. Examples are: the purchase of luxury assets, financial investments, investing in gaming companies or commercial investments.

Most of the people think that money laundering refers to funds acquired with drugs trafficking, but there are many predicate offences for ML such as human trafficking, arms trafficking, robbery, fraud, corruption, kidnapping and tax crimes.

Financing of Terrorism

Financing of terrorism (FT) is the financing of terrorist acts, of terrorists and terrorist organizations. A terrorist act is an act to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act. The most basic difference between financing of terrorism and money laundering involves the origin of the funds. FT uses funds for an illegal political purpose, but the money is not necessarily derived from illicit proceeds. Money laundering always involves the proceeds of illegal activity. There is a need for the terrorist group to disguise the link between it and its legitimate funding sources. In doing so, the terrorists use methods similar to those criminal organizations use to launder

money like cash smuggling, structuring, wire transfers, purchase of monetary instruments, use of debit and credit cards. While ML is concerned with obscuring the source of funds, FT is mostly concerned with obscuring the end recipient of the funds.

Financing of Proliferation of Weapons

Financing of proliferation (FP) is the provision of funds 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.

AML/CFT/CFP systems

Primary Legislation Governing AML/CFT/CFP in Curaçao

The Company shall comply with the Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction¹ (Regulation) issued in the implementation of NOIS, NORUT, Sanctions National Ordinance and Kingdom Sanctions Act. In addition, the following legal acts are relevant to the Company's activity (non-exhaustive list):

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92) (hereinafter – NOIS)²;
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99) (hereinafter – NORUT)³;
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators, as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73)⁴;

¹ https://gamingcontrol.spin-cdn.com/media/aml_cft/20240527_regulations_for_the_combating_of_money_laundering_and_financing_of_terrorism_versie_final_20052024.pdf

² NOIS: https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2017_no_92_landsverordening_identificatie_bij_dienstverlening_gt.pdf

Amendments of NOIS: https://gamingcontrol.spin-cdn.com/media/aml_cft/20240517_pb.pdf

³ NORUT: https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2017_no_99_landsverordening_melding_ongebruikelijke_transacties_gt.pdf

Amendments of NORUT: https://gamingcontrol.spin-cdn.com/media/aml_cft/20240517_pb.pdf

⁴ Indicators for recognizing unusual transaction: https://gamingcontrol.spin-cdn.com/media/pdf_files/20191108_pb_2015_no_73_regeling_indicatoren_ongebruikelijke_transacties.pdf

- Sanctions National Ordinance (N.G. 2014, no. 55)⁵;
- Kingdom Sanction Act (N.G. 2016, no. 54);
- National Decree entering into force of Kingdom Sanction Law (N.G. 2017, no. 2);
- National decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of United Nations' Security Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29)⁶;
- National Decree for general measures, of the 10th July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the United Nations' Security Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28)⁷;
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006), 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions Decree People's Democratic Republic of Korea 2015) (N.G. 2015 no. 30)⁸;
- National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34)⁹;
- The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

Company firmly believes that a reputation for integrity and openness, both in its business model and in its management systems and procedures - are crucial to achievement of its commercial goals and plans, and also to the fulfilment of its corporate responsibilities. The Company is, therefore, committed to the highest standards of AML/CFT/CFP measures in its operations, and it adheres to both established and recommended international standards to prevent the use of its services for the above purposes.

Amendment of the Indicators for recognizing unusual transactions:: https://gamingcontrol.spin-cdn.com/media/aml_cft/20240611_60_mrmaw_tot_wijz_regeling_indicatoren_ongebruikelijke_transacties_1.pdf

⁵ Dutch version of UNSC Resolutions: https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2014_55_sanctions_national_ordinance.pdf

English versions of UNSC Resolutions can be found here: <https://main.un.org/securitycouncil/en>

⁶ https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2015_29_sanction_decree_al_qaida_taliban_isil_anf_etc.pdf

⁷ https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2015_28_sanction_decree_libya.pdf

⁸ https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2015_30_sanction_decree_dpr_of_korea_2015.pdf

⁹ https://gamingcontrol.spin-cdn.com/media/pdf_files/20190422_pb_2018_34_continuance_pbs_2015_28_29_30.pdf

Supervisory Authorities

For the purpose of compliance with AML/CFT/CFP legislation and regulation, casinos and providers of other online games registered in Curaçao are supervised by the state authority with the following details:

- name: Curaçao Gaming Control Board (GCB);
- address: Emancipatie Boulevard, Dominico F. "Don" Martina 23, Willemstad, Curaçao;
- phone: +(599 9) 737-2299;
- email: info@gcb.cw.

For the purposes of unusual transaction reporting, the Curaçao Financial Intelligence Unit with below details; acts as an independent buffer between the private sector and the criminal justice system, in the joint combat against ML, FT and FP:

- name: Curaçao Financial Intelligence Unit (FIU);
- address: Emancipatie Boulevard, Dominico F. "Don" Martina 23, Willemstad, Curaçao;
- phone: + (599 9) 462 6588;
- emails: info@fiucuracao.cw.

Effective Controls

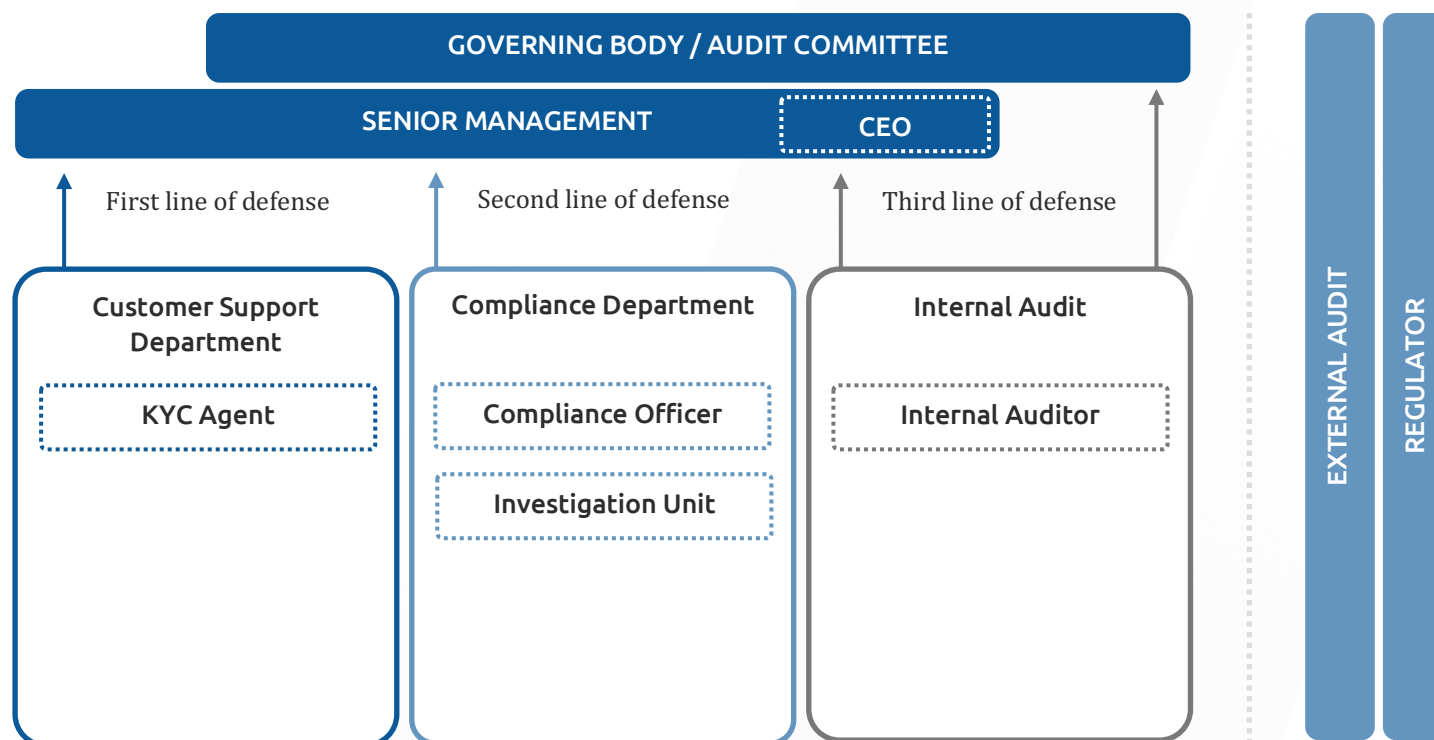
To ensure proper implementation of AML/CFT/CFP procedures and controls, Company has effective controls covering:

- effective AML/CFT/CFP compliance program;
- senior management oversight;
- appointment of the Compliance Officer and other employees with certain responsibilities;
- compliance and audit function;
- staff screening and training.

The senior management of the Company is responsible for managing the business effectively and for the oversight of internal AML/CFT/CFP controls and systems. The senior management appoints the Compliance Officer who has overall responsibility for the establishment and maintenance of Company' AML/CFT/CFP systems and is the central reference point for suspicious transaction reporting.

Three Lines of Defense

The Company follows the three lines of defense framework when managing ML/FT/FP risks. The three lines of defense is an industry model for managing risk. It is used to structure roles, responsibilities and accountabilities for decision making, risk and control management, and independent assurance. The three lines of defense are used as the fundamental guiding principle when performing the AML/CFT/CFP obligations.



Senior Management Responsibilities

The Company's Senior Management responsibilities include but are not limited to:

- maintaining compliance with effective laws of Curaçao;
- monitoring and overseeing the compliance activities of the Company to ensure they are in accordance with the applicable laws, regulations and internal policies and procedures;
- reviewing the AML/CFT/CFP Policy to ensure it is comprehensive, adequate and viable;
- approving the AML/CFT/CFP Policy;
- ensuring that the AML/CFT/CFP Policy is effectively implemented by the Company's Compliance Officer and other employees;
- Designating a qualified employee to serve as the Company's Compliance Officer;
- Reviewing the performance of the Compliance Officer and assign responsibility to such person to maintain and monitor overall compliance on a day-to-day basis with AML/CFT/CFP requirements;
- Ensuring that the Compliance Officer has sufficient authority and resources (monetary, physical and personnel) to administer an effective AML/CFT/CFP Policy based on the Company's risk profile;
- Periodically receiving and reviewing reports presented by the Compliance Officer to ensure that AML/CFT/CFP Policy is being executed as approved and that it is, in fact, serving its intended purpose of maintaining the integrity, safety and soundness of the Company;
- Annually reviewing changes proposed to be made to AML/CFT/CFP Policy, and, if satisfied that the modifications are desirable, approving the modifications/changes;
- Designating and contracting the services of a competent entity to perform independent compliance audits of the Company to test for the Company's level of adherence to the applicable AML/CFT/CFP laws and regulations.

KYC Agents

KYC Agents comprise the first line of defense, which is a part of the risk management system that is related to the structural units with whose activities risks are associated and that must identify and assess these risks, their specific features and scope and that manage these risks by way of their ordinary activities, primarily by way of application of due diligence measures.

The first line of defense must have good knowledge of the customer and the specific features of their activities and business activities.

Principal functions of the KYC Agents include in particular:

- performing of the customer's onboarding procedure (as defined below) and application of CDD/EDD measures before the establishment of the Business Relationship with the Customer;
- performing of the ODD/EDD measures in the course of the established Business Relationship with the customer (incl. the monitoring of transactions and periodically updating the Customer's information);
- identifying transactions in the customer's activities that are suspicious or unusual or do not correspond to reasonable economic objectives, or transactions that refer to such circumstances, and referring such transactions to the second line of defense (Compliance Department) for analysis and if necessary, directly to the senior management;
- perform other functions which are assigned to the KYC Agents under the applicable law, internal policies, job description

Compliance Department

Compliance Officer

The Company shall formally designate a senior officer at management level and independent from the games operations, responsible for the detection and deterrence of ML/FT/FP (hereinafter – the Compliance Officer) using the **decision for the Compliance Officer appointment** (annex 2). The Compliance Officer acts as the focal point within the Company for the oversight of all activities relating to the prevention and detection of ML/FT/FP and providing support and guidance to the senior management to ensure that ML/FT/FP risks are adequately managed. The Compliance Officer shall be assigned at least the following responsibilities:

- to design and implement the AML program;
- to verify adherence to local laws and regulations regarding the detection and deterrence of ML, FT and FP;
- to review compliance with the Company's policy and procedures;
- to organize training sessions for the employees on various compliance-related issues;

- to analyze transactions and verify whether any are subject to reporting according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions;
- to review all internally reported unusual transactions for their completeness and accuracy with other sources;
- to keep records of internally and externally reported unusual transactions;
- to execute closer investigation of unusual transactions if necessary;
- to prepare the external report of unusual transactions;
- to make necessary changes to the AML program;
- to remain informed on the local and international developments on ML, FT and FP and to make suggestions to management for improvements; and
- to prepare periodic information on the Company's efforts against ML, FT and FP.

The above-mentioned responsibilities shall be included in the job description of the Compliance Officer. The job description shall be signed off and dated by the Compliance Officer, indicating his/her acceptance of the entrusted responsibilities. The Compliance Officer must have timely access to customer identification data and other CDD information, transaction records, and other relevant information. The Compliance Officer must be able to act independently.

Investigation Unit

Investigation Unit works Under the auspice of the Compliance Officer. The following functions shall be performed by the Investigation Unit:

- assistance of the Compliance Officer regarding reviewing received internal disclosures and exception reports;
- assistance of the Compliance Officer regarding external report of unusual transactions;
- perform other functions which are assigned to the Investigation Unit under the internal policies and job description.

Audit Function

Audit function shall be established to perform regularly reviews of the AML/CFT/CFP systems to ensure their effectiveness. The frequency and extent of the review should be commensurate with the risks of ML/FT/FP and the size of the Company's business, as well as regulatory requirements. Where appropriate, Company will seek a review from external auditors.

Independent audit functions include the following principles:

- compliance and audit functions are independent in practice;
- the regular review is performed at a frequency of **once a year**;
- adequately resourced internal audit department or an outside independent party is leveraged to perform the auditing;
- availability of direct communication to senior management through regular committees (compliance committee) or other means of direct communication.

The performing of audit functions shall be ensured by the decision of senior management, which should be adopted, **at least, on an annual basis**.

Risk Based Approach (RBA)

Based on the FATF Recommendations, the Company shall apply a risk-based approach (hereinafter – RBA) when designing policies, procedures and controls to combat ML, FT and FP. By adopting a RBA, the Company is able to ensure that measures to prevent or mitigate ML, FT and FP are commensurate with the risks identified. That means the higher the risk, the more measures the Company has to take to mitigate the risk. Where the risks are lower the Company may take simplified measures, provided that this is consistent with the country's assessment of its ML, FT and FP risks.

Applying Risk-based Approach means that the Company shall:

- assess the risks that ML/FT/FP may occur within the Company beforehand;
- design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;

- monitor and improve the effective operation of these policies, procedures and controls;
- document the risk assessments, including everything that has been done and the reason for this being done.

The Company document their policies, procedures and controls relative to their applied RBA. Since risks are dynamic, the Company must, on an on-going basis, monitor the effective operation of the policies, procedures and controls concerning their RBA and, when needed, make the necessary amendments to these policies, procedures and controls. The risk assessment should also be made available to the GCB upon request.

Business Risk Assessment

The Company shall carry out a business risk assessment (hereinafter – BRA) to identify the ML/FT/FP risks the Company is exposed to and ensure that the policies, controls and procedures adopted are adequate to prevent and mitigate those risks. The risk assessment should address the ways in which the Company's products and services could be used for ML, FT and FP and the extent of the risk that this will happen. All factors that may have an impact on the risks of ML, FT and FP must be taken into account in the risk assessment, but special consideration must be given to the type of customers, products and services offered, delivery channels and geographical risk factors. Once the BRA has been conducted, the Company can set a risk appetite: it decides how much risk it is prepared to accept.

The Company shall revise their BRA whenever there are changes to the environment within which they are operating and within their business activities, such as introduction of new payment methods, new markets, new games or regulatory changes. The assessment of risks related to technological developments shall be carried out prior to launch of new products, business practices, delivery mechanism or new technologies. In the absence of changes, the Company shall assess their business risk **at least annually**, to evaluate whether any changes thereto are necessary.

The aspects of the BRA should cover include:

- the methodology adapted;
- the reasons for considering a risk factor as presenting a low, medium or high risk;
- the outcome of the BRA;
- any information sources used.

The BRA Report of the BRA carried out shall be added as an annex to the AML/CFT/CFP Policy (annex 3).

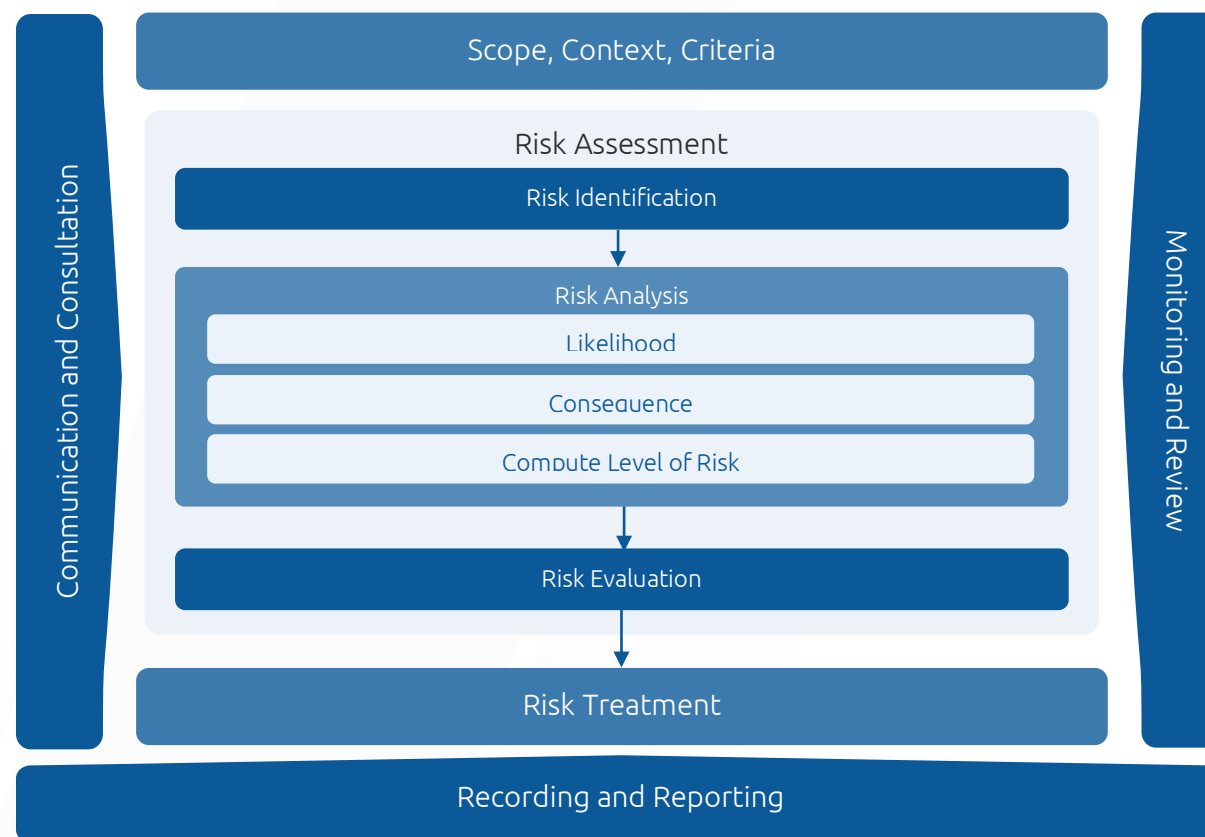
In order to work risk-based, it is also important that the Company continuously follows the latest reporting requirements regarding ML, FT and FP.

Risk Management Process

The Company prepares and regularly updates the risk assessment in order to identify, assess, analyze and manage ML, FT and FP risks. The process of risk assessment, executed by the Company shall include at least the following stages:

- risk factors identification;
- risks factors analysis;
- risks factors evaluation.

Risk assessment is an integral part of the risks management process within the RBA. The risk assessment has to be documented and approved by the **board of directors** of the Company. It should also be made available to the GCB upon request.



In the course of risk assessment, the Company uses at least the following sources:

- applicable regulatory requirements (Curaçao laws, decrees, etc.);
- last national risk assessment of the jurisdictions where they operate;
- last supra-national (UN-wide) risk assessment;
- guidelines of authorities (incl. international organizations);
- the knowledge previously obtained when performing activities similar to the Company.

The Company assess the ML/FT/FP risks of its customers by assigning a ML/FT/FP risk rating taking into consideration the risk categories as specified below.

After the initial risk assessment has been performed, the Company shall continuously and regularly, **at least on annual basis**, assess the effectiveness of the measures implemented, the need for the implementation of additional measures and the resolution of any incidents and their consequences in the course of carrying out the subsequent risk assessments. The monitoring process may include:

- review of the CDD/EDD/ODD procedures;
- ongoing assessment and testing of the customer identification measures and business relationship monitoring rules and alerts;
- review of suspicious activity reports, internal escalations, and compliance incidents;
- review of regulatory updates, typologies, and external risk indicators that may impact the Company's risk exposure.

Additionally, the internal audit of the AML/CFT/CFP Policy described herein systematically assesses the effectiveness of the measures to mitigate risks, their functioning as intended and the appropriateness of the risks and the control arrangements.

Customer Risk Assessment

The customer specific risk assessment (hereinafter – CRA) has to be carried out either **prior to the carrying out of an occasional transaction, or during establishing a business relationship**. It is possible that this initial customer specific risk assessment will have to be revised at a later stage of the business relationship and this may result in a customer's risk rating having to be adjusted.

The CRA will assess the particular risks the Company will be exposed to when providing its services or products to customers. The information collected to draw up the CRA will formulate the customer's risk profile. On the basis of the CRA, the proper level of CDD can then be applied.

Determination of the customer's risk profile

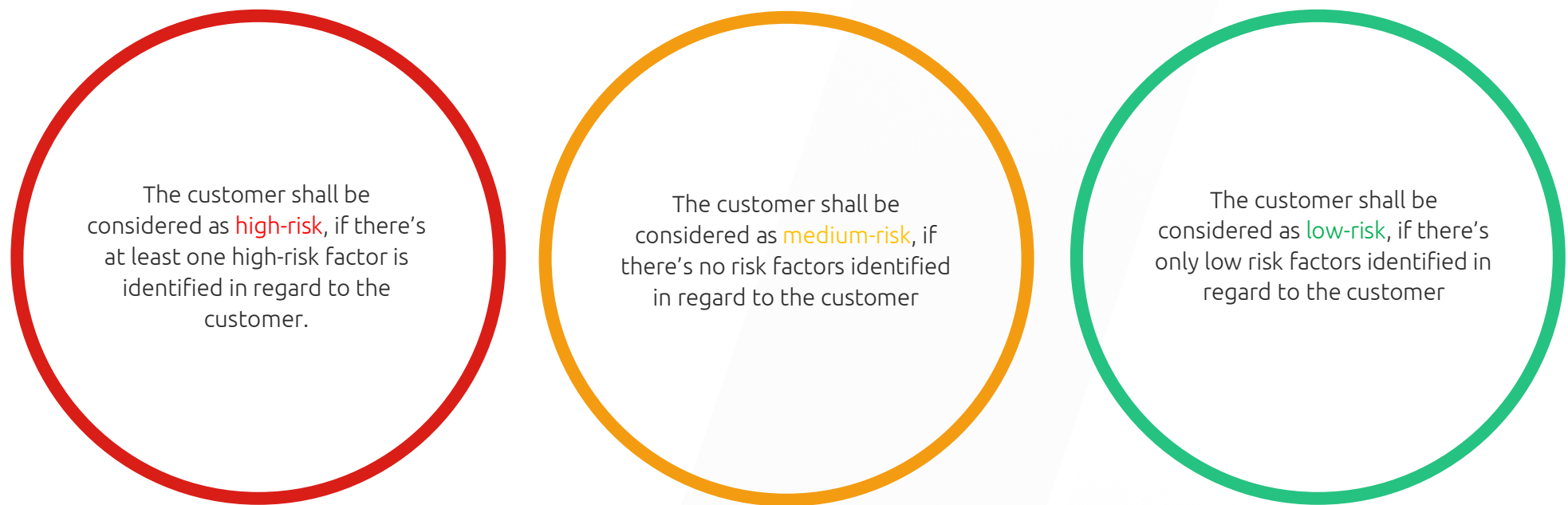
The KYC Agent shall analyse the data obtained during the implementation of CDD/EDD measures, compare the aforementioned data with risk factors identified in the risk assessment for each ML/TF risk category and determine the customer's risk profile in accordance with the following.

The Company establishes and maintains the **List of Risk Factors** as a separate document (annex 4), based on the BRA carried out, which contains the list of risk factors and their risk scores that shall be taken into account when establishing the individual customer's risk profile.

For the each of aforementioned risk categories, the following risk score may be identified:

- **Low risk (1 point)** – no influential risk factors exist in risks category, the customer itself and the Customer's activities are transparent and do not deviate from the usual activities, i.e. the activities of a reasonable and average person, in that field of activity, and there is no suspicion that the risk factors as a whole could lead to the realization of the risk of money laundering or terrorist financing;
- **Medium risk (2 points)** – one or several risk factors exist in the risks category that deviate from the usual activities of a person acting in that field of activity, but the activity is still transparent and there is no suspicion that the risk factors as a whole could lead to the realization of the risk of money laundering or terrorist financing;
- **High risk (3 points)** – one or several risk factors exist in the risks category that as a whole raises suspicion of the transparency of the Customer and their activities, which causes the person to deviate from persons usually acting in that field of activity and it is at least possible that money laundering or terrorist financing is taking place;
- **Prohibited risk (4 points)** – risk is not acceptable by the company due to the risk tolerance established.

Each risk category shall be assessed in accordance with the risk factors identified for the customer.



Maintaining of the customer's risk profile

The Company reviews the business relationship with each customer as per the schedule below to ensure if the risk profile determined is still applicable or should be modified based on any changes of the identity of the customer, the nature of the customer's economic activity, the customer's country of residence, the actual volume of transactions and other facts, which may affect the CRA. Only the Compliance Officer is permitted to alter a customer's risk profile. The Compliance Officer will maintain relationship opening documentation, activity statements, and other necessary documentation to support the risk profiles assigned to customers.

Low Risk

The Compliance Officer will engage in annual reviews of each low-risk customer.

Medium Risk

The Compliance Officer performs annual reviews of every medium-risk customer that is no longer a new relationship (i. e. every 6 months after the customer's onboarding).

High Risk

Due to the high-risk nature of these relationships, the Compliance Officer performs monthly reviews of every high-risk customer including a transactional review.

Each high-risk customer will require EDD before the conclusion of business relationship and additional facts will be gathered to learn more about the customer.

Non-acceptable customers

The Company has created the list of prohibited risk factors (annex 4) in the presence of which the customer will not meet the Company's risk appetite. In case, when such risk factor has arisen in the course of the customer's onboarding or before making occasional transaction – the Company refuses to establish the business relationship or perform transaction with such customer. If prohibited risk factor is identified in the course of the business relationship established – such relationship shall be terminated in accordance with this Guideline.

The Company may not establish a business relationship or conduct a transaction and shall terminate the business relationship where the customer does not facilitate compliance with the relevant due diligence measures.

Anonymous accounts

The Company is prohibited from keeping anonymous accounts or accounts in obviously fictitious names. The Company must identify the customer and ask for the customer's name and other relevant information to determine the purpose and nature of the business relationship. Without sufficient knowledge, the Company may not establish or maintain a business relationship or carry out occasional transactions

Prohibited countries

Curaçao prohibits for its own residents to access Curaçao-based online gaming operators. Additionally, the Company cannot accept customers from territories as determined by the GCB from time to time. There are countries that have treaties in place with Curaçao that include restrictions prohibiting persons from such countries to access to Curaçao-based online gaming operators.

Inability to complete CDD

Where unable to comply with the CDD requirements the Company must not open the account, commence business relations or perform the transaction. If the Company already has a business relationship with the customer the Company should terminate the business relationship.

The Company has to make an unusual transaction report to the FIU if presumption of ML/FT/FP exist.

Risk Factors Specific to the Gambling Sector

There are four risk areas that the BRA and CRA have to cover. These are:

Customer risk

Customer risk is the risk of ML/FT/FP that arises from maintaining relations with a given customer. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. Categories of customers' whose activities may indicate a higher risk include:

- customers who have multiple sources of income;
- customers with irregular income streams;
- PEPs;
- high spenders (money can be derived from illegal activities);
- disproportionate spenders (inconsistent with casino's information about customer's known source of income/assets);
- casual customers like locals/tourists, especially when spending pattern changes;
- improper use of third parties, criminals use third parties to gamble to break up large amount of cash, to buy chips or to cash out on behalf of others to avoid CDD measures;
- multiple casino customer rating accounts to hinder a casino to track their gambling activities;
- unknown customers (redeeming large amounts of chips);
- junkets (junket operators monitor customer activity and issues and collect credit).

The Company must set a value which represents the upper value of a typical customer's transactions.

Geographical risk

The geographical risk is the risk posed to the Company by the geographical location of the Company itself, the customer and the source of wealth of the business relationship. The nationality, residence and place of birth of the customer have to be taken into account as well as these might be indicative of a heightened geographical risk. It is advisable to take into account a variety of sources of information, including:

- countries on the FATF list of High - Risk Jurisdictions subject to a Call for Action;
- countries on the FATF list of Jurisdictions under Increased Monitoring;

- countries on the CFATF Public Statement;
- countries identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR);
- countries on the European Commission's list of third countries having strategic deficiencies in their AML/CFT/CFP regime;
- countries sanctioned by the OFAC;
- countries identified by credible sources as providing funding or support for terrorist activities or have terrorist organizations operating within them;
- countries on the Corruption Perception Index compiled by Transparency International.

Product, service and transaction risk

Some products or services are inherently riskier than others and are therefore more attractive to criminals. These include products or services which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it individually or in collusion with others. The use by customers and the acceptance by the Company of specific payment methods, which are considered to present a higher risk of ML/FT, should also be treated as high risk factors. These include:

- proceeds of crime – risk that money transferred is derived from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking and theft from employer;
- anonymous payment methods such as pre-paid cards and virtual assets;
- use of casino accounts – this should only be done for gambling purposes and not to deposit and withdraw without gambling or minimal play;
- types of specific games (e.g. roulette, craps → even bets);
- peer to peer gaming;
- the use by customer of accounts held or cards issued in the name of third parties;
- the transfer of funds from one gaming account to another;
- types of financial services (credit/marker, currency exchange, check cashing);
- multiple casino accounts or wallets (internet operator may own and control multiple web sites);
- changes to financial institution accounts to fund casino account;

- identity fraud - details of stolen financial institution accounts or stolen identities used to successfully open financial institutions accounts and used on web sites;
- using cash to fund a pre-paid card poses similar risks as cash;
- games involving multiple operators (poker on platforms shared by multiple operators);
- electronic wallets (e- wallets) - not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. Also, e-wallets which only accept money from financial institution accounts; the financial institution issued statements may only record the payment to the e-wallet, not the transaction to the Internet casino. This may be useful for dishonest customers who wish to disguise their gambling.

Distribution channels risk

The channels through which the Company establishes a business relationship or through which transactions are carried out may also have an impact on the risk profile of a business relationship or a transaction, including:

- channels that Favor anonymity increase the risk of ML/FT if no measures are taken to address the risk;
- non-face-to-face interactions - while situations where interaction with the customer takes place on a non-face-to-face basis no longer lead to the relationship being considered as automatically high risk, interacting in this manner is still to be considered as a high risk factor for risk assessment purposes unless the Company adopts technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations;
- involvement of a third party in the interactions between the customer and the Company. This is especially the case where these third parties are not themselves subject to any form of AML/CFT/CFP obligations.

Technological developments risk assessment

The Company shall also maintain appropriate procedures and controls for preventing the misuse of technological developments for the purpose of ML/FT/FP. The Company shall identify and assess the ML and T risks that may arise whenever:

- a new product is developed;
- a new business practice emerges;

- a new delivery mechanism becomes available;
- a new or developing technology is used for both new and pre-existing products.

Customer Acceptance Policy

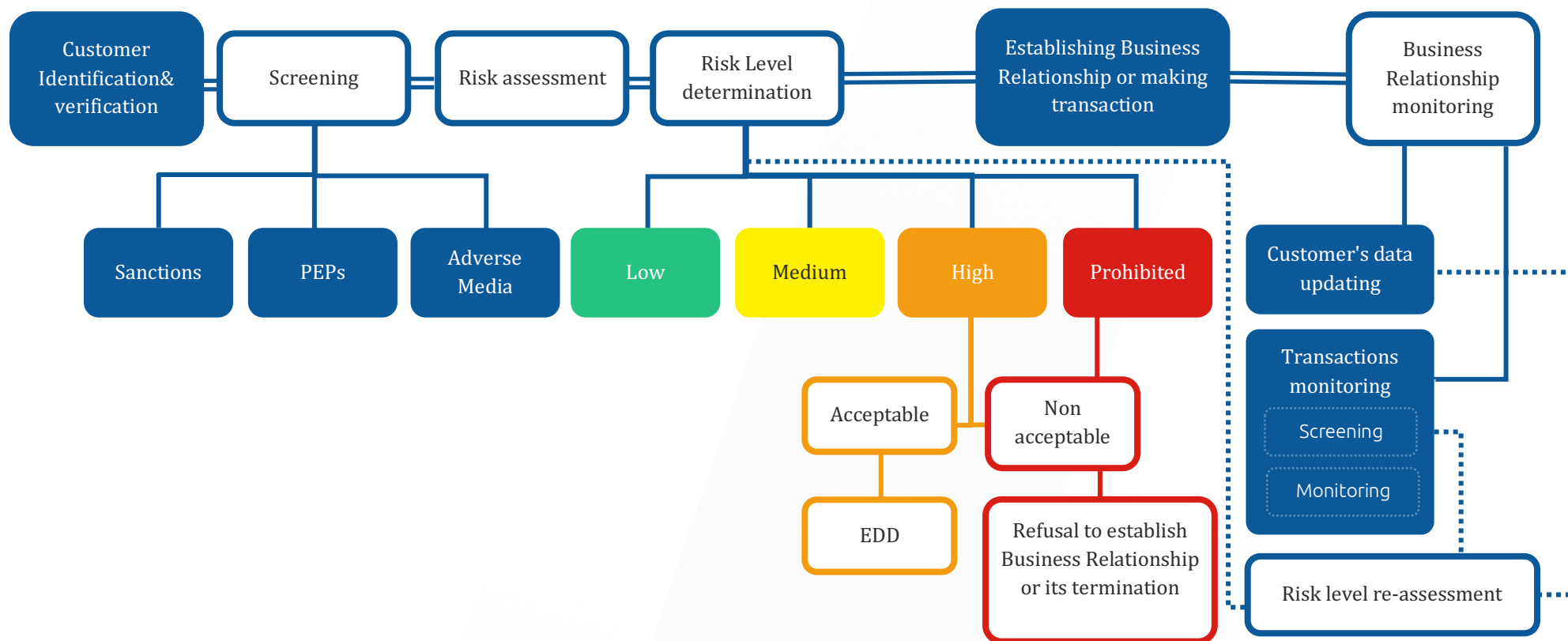
On the basis of the CRA, the proper level of CDD can then be applied as stipulated in the Customer Acceptance Policy.

Any unusual behavior needs to be reported to the FIU. If FIU, after proper analysis of an unusual transaction, concludes that there is a suspicion of ML and/or TF, this transaction will be reported to the Public Prosecutor's Office as a suspicious transaction.

Customer Due Diligence

Customer due diligence (CDD) is central to an effective AML/CFT/CFP regime. The Company takes CDD measures to identify and verify each of its customers so it can:

- determine the money laundering and terrorism financing risk posed by each customer;
- decide whether to proceed with a business relationship or transaction;
- assess the level of future monitoring required.



The **CDD measures** to be taken are as follows:

1. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information;
2. Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that the Company is satisfied that it knows who the beneficial owner is.
3. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;

4. Conducting ODD on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the customer, its economic activity and risk profile, including, where necessary, the source of funds.

Timing of CDD Measures and Minimum Requirements

The Company has the obligation to undertake CDD measures when:

- when customer engages in financial transactions equal to or above NAF. 4,000;
- carrying out occasional transactions above the monetary equivalent of NAF. 4,000;
- there is a suspicion of ML/FT/FP; or
- the Company has doubts about the veracity or adequacy of previously obtained customer identification data.

All CDD measures must have been conducted at the time the NAF. 4,000 threshold is reached. The threshold is to be **calculated on a daily basis taking into account all deposits and withdrawals made by the customer since the establishment of the business relationship**, including any peer-to-peer transfers. In carrying out the CDD measures, customers may be allowed to continue using their gaming account while the Company obtains any necessary information from the customer concerned. However, if the NAF. 4,000 threshold is reached, the customer shall be prohibited from depositing funds into the account or withdrawing funds from the account. If the requested information and documentation is not received **within 30 days from the moment the NAF. 4,000 threshold was met** in order for the Company to complete CDD, the Company has to **terminate the relationship** with the customer and **report the transaction to the FIU if presumption of ML/FT/FP exists**.

The Company is required to apply a **minimum level of CDD measures** prior to reaching the NAF. 4,000 thresholds. Thus, simultaneously with the opening of an account, the Company must identify the customer by collecting the minimum personal details, including:

1. name and surname;
2. permanent residential address; and
3. date of birth.

The Company must also conduct the sanctions screening simultaneously with the opening of an account.

Identification and verification of the customer

Identification refers to the collection of personal details of the customer to establish the identity of the customer. Verification of an identity refers to actions taken to verify that the customer exists and is who the customer claims to be. Verification consists in confirming the information collected for identification purposes using reliable, independent source documents, data or information. The personal information required and extent of verification to be carried out, will vary depending on risk.

When identifying the customer, at a minimum the following information must be collected:

- full name;
- permanent residential address;
- date of birth;
- place of birth;
- nationality; and
- identity number.

The Company shall carry out a CRA in order to have sufficient information available to detect unusual activity in the course of the business relationship. A provisional risk rating will be assigned based on the initially collected information. This is revised once questions are answered, or additional information received. On the basis of the CRA, the proper level of CDD can be applied.

Verification of identity is carried out by making reference to an **unexpired government-issued document containing photographic evidence of the customer's identity** (e.g. passport, identity card), including:

- driver's license;
- identification card;
- travel document or passport.

Where such a document does not allow verification of the customer's residential address, the Company obtains an another document **not older than 6 months**, to verify the residential address, including:

- bank statement;
- utility bill;
- correspondence from a central or local government authority, department or agency;
- rental or lease agreement.

Other verification methods which may be applied by the Company include:

- contacting the customer by letter, e-mail or telephone to verify the information supplied;
- sending a verification code to the e-mail address to verify that the address is current and genuine;
- checking social media, telephone directories, companies' registries or media and news sources;
- Biometric checks to confirm that the individual providing the document is the one described therein;
- cross referencing the information in the Company's possession with geo-location information, IP address data, funding method data etc.

Verification is carried out for the Company to determine to its own satisfaction that the customer is who he declared himself to be. What is important is that documents are clear, legible and of good quality. Verification of evidence of identity implies a check whether the document presented is **authentic, clear, legible, legitimate, of good quality and that it has not been stolen from the true owner**. If the Company obtains foreign documentation, extra care should be taken with regard to verifying its authenticity, particularly where the type of document is unfamiliar.

If the customer is not physically present for identification, the identification and verification shall be carried out taking into account the specific risks associated with business relationships or transactions without personal contact.

Where the Company does not have sufficient comfort that it knows its customer, the Company shall take additional measures to do so. Some of these measures include requesting additional identification documents, asking the customer to provide a photo of himself holding the ID, requiring a first payment through an account held in a reputable jurisdiction, using systems which generate codes for transmission to customers through a verified mobile phone and requiring it to be returned.

Identification and verification of the Beneficial Owner

The Company shall make sure that customers are registering an account to play and transact on his/her own behalf. For this purpose, the Company includes a specific wording in the terms and conditions that the customer must explicitly accept, together with a declaration in the form of a tick box that the customer is registering to play on his/her own behalf. The Company has to ensure that their ongoing procedures allow for the detection of possible instances where the customer is actually playing on behalf of third parties.

In an instance where funds being wagered are collected from multiple persons who will eventually share in any winnings, the particular transaction will not only be considered as having been undertaken by the customer but undertaken also for the benefit of those persons providing the necessary funding. These persons are considered as beneficial owners and the Company has to identify them and verify their identity.

Obtaining information on the Purpose and Intended Nature of the Business Relationship

The Company should understand why a prospective customer is seeking to acquire a specific service or product from the Company. Within the context of the gambling sector, the purpose behind the opening of a gaming account is quite self-evident for which it is not required to obtain any additional information from their customers. However, this CDD measure also requires the development of a customer risk profile to have sufficient information available to allow the detection of unusual activity in the course of a business relationship.

To this end, the Company has to collect sufficient information and, where it is necessary, documentation to establish a customer's **source of wealth as well as the expected level of activity**. As to the extent of the information that the Company is to collect, it is essential that this reflects the level of ML/FT risk identified through the customer risk assessment. Where the risk is not high, a **declaration from the customer with some details** (e.g. nature of employment/business, usual annual salary etc.) can be sufficient. **Social media** can also be used as a source of information. Where the risk of ML/FT is higher or the Company has doubts as to the veracity of the information collected, the information obtained would need to be substantiated by independent and reliable information and documentation.

In developing a customer risk profile, the Company may also consider using statistical data to develop behavioral models against which to eventually gauge a customer's activity rather than collect source of wealth information. Where the Company opts to adopt this approach, it can use data collected from a relevant central statistics department, such as average national income, average disposable income etc. These indicators should allow the Company to determine the average wagering power of customers from a given jurisdiction. The Company can also use data collected over a

period of time by the Company itself, which allows to create the profile of an average customer. It is important to note that the reference is not to the statistical data on the individual customer but to statistical data obtained from a range of customers. The Company should therefore only use this specific alternative where their customer-base is wide enough to allow the creation of an average profile. New casinos would therefore not be expected to use this method unless they are able to obtain gaming data from another casino offering the same games within the same markets and having a similar business model to the one being adopted by the new casino.

It is important to note that the use of statistical data is incompatible with high-risk situations as the transactional pattern will fall outside the average behavioral model. In such circumstances, the Company would have to collect source of wealth information as set out above.

Politically Exposed Persons identification

Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country and the direct family members or close associates of such persons. Examples are:

- Heads of State or of government;
- senior politicians;
- senior government;
- judicial or military officials;
- senior executives of state-owned corporations;
- important political party officials.

Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions. Examples are:

- Heads of State or of government;
- senior politicians;
- senior government;
- judicial or military officials;
- senior executives of state-owned corporations;

- important political party officials.

Persons who are or have been entrusted with a prominent function by an international organization refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.

The Company shall take reasonable measures to determine whether a customer is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. Screening for PEP status has to be carried out before establishing the business relationship or conducting the occasional transaction. In addition, the Company must regularly screen for PEP status during the business relationship. For PEP status screening the Company relies on internet search and/or consults the relevant reports and databases.

Reliance on Third Parties and Outsourcing

The Company may rely on third parties when performing elements 1.-3. of the CDD measures in chapter “Customer Due Diligence” above, provided that the criteria set out below are met. The third party should be subject to CDD and record-keeping requirements. The third party will have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the Company. Where such reliance is permitted, the ultimate responsibilities for CDD measures remain with the Company.

The criteria for the third party to be met are as follows:

- The Company has to obtain the information concerning elements 1.-3. of the CDD measures immediately from the third party it is relying upon.
- The Company should have an agreement with the third party being relied upon that copies identification data or other relevant documentation relating to CDD requirements will be made available upon request and this arrangement must be tested from time to time to ensure that it actually functions as set out in the agreement. The Company, however, remains responsible for the carrying out of a customer-based risk assessment, determining whether the customer is a PEP and conducting ODD.
- The Company should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and recordkeeping requirements as described in this regulation. The third party will have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying institution, and would apply its own procedures to perform CDD measures.

- When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

It must be noted that the situation is different for the outsourcing/agency scenario, in which the outsourced entity applies the CDD measures on behalf of the Company, in accordance with its procedures, and is subject to the Company's control of the effective implementation of those procedures by the outsourced entity. It is important that the Company is aware that it will remain responsible at all times for compliance with said regulations. For this reason there should be periodical assessments of how the outsourced entity is fulfilling its obligations under the outsourcing arrangement both quantitatively as well as qualitatively. However, the decision whether to on-board a customer or to continue a business relationship on the basis of risk cannot be outsourced.

Any activity performed by an agent or group company is to be considered as an activity performed by the Company. As such, any customer on-boarded by the agent or group company has to undergo the same checks and controls as customers on-boarded by the Company itself. It is therefore up to the Company to ensure that its AML/CFT/CFP controls, policies, measures and procedures are applied by the agent or group company.

Simplified Due Diligence

Where the risks of ML/FT/FP are lower, the Company may conduct SDD, which should take into account the nature of the lower risk.

In low-risk scenarios the Company may limit identification to the following information:

1. full name;
2. permanent residential address;
3. date of birth;

Examples of other possible measures:

- verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;

- the extent of verification may also vary depending on the risk posed by the particular business relationship. In a low-risk situation, the Company can also use alternative reputable information sources, even where these do not contain photographic evidence of the customer's identity (e.g. birth certificates, bank statements etc.);
- the extent of personal details verified can also vary. In low-risk situations, the Company has to verify the basic identification details, while the verification of any other personal details is upon the Company, as long as it has sufficient comfort that it knows who its customer is;
- reducing the frequency of customer identification updates;
- reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold.

SDD measures are not acceptable whenever there is suspicion of ML/FT/FP, or where specific higher-risk scenarios apply.

Enhanced Due Diligence

In circumstances where risk of ML/FT/FP is higher, EDD measures have to be taken to mitigate the increased risk. The EDD measures should be consistent with the risks identified. In particular, the Company should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual.

High risk circumstances refer, among other things to:

- residents of higher risk geographic areas;
- Political Exposed Persons (PEP's);
- products or transactions that might favor anonymity;
- new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

Examples of EDD measures include:

- obtaining additional information on the customer, like occupation, previous address and information available through public databases, internet, etc.;

- obtaining additional information on the intended nature of the business relationship;
- obtaining information on the source of funds or source of wealth of the customer.
 - source of funds information has to be requested from time to time even though there may not be any change in pattern or activity conducted by the customer;
- obtaining information on the reasons for intended or performed transactions;
- obtaining the approval of senior management to commence or continue the business relationship;
- conducting enhanced ODD;
- requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

Politically Exposed Persons

The Company is required, in relation to foreign PEPs, (whether as customer or beneficial owner) in addition to performing normal customer due diligence measures, to:

1. have appropriate risk-management systems to determine whether the customer or the beneficial owner is a PEP;
2. obtain senior management¹⁰ approval to service the PEP (for establishing the business relationship for new customers, continuing the business relationship for existing customers or for conducting the occasional transaction);
3. take reasonable measures to establish the source of wealth and the source of funds. The investigation must then determine whether the customer's spending pattern matches his legal source of funds. The Company requests a statement from the customer about the source of funds and verifies them by consulting independent and reliable sources. Depending on the risk in specific cases, this can in the first place be public sources. When public sources cannot, or can insufficiently verify the received information, the Company can request the customer to provide documents; and
4. conduct enhanced ongoing monitoring of the business relationship.

¹⁰ senior management are the persons who determine the day-to-day operations or those directly below the level of those determining the day-to-day operations. The approval can also be from the manager of the Compliance department

Although EDD is required for each PEP, the measures do not have to be the same for every PEP. In cases of a higher risk business relationship with such persons, the Company is required to apply the measures referred to in points 2.-4. above. Should a customer who had not been identified as a PEP at on-boarding stage result to have become one, the Company is required to implement the measures described above within the **30-day window**. If the measures cannot be successfully applied within the specified time period, the Company shall terminate the relationship with this customer.

The measures are tailored to the risk of the PEP, where the following is taken into consideration:

- the type of public function of the PEP;
- the country from which the PEP originates;
- the transactions that the PEP carries out.

The requirements for all types of PEP should also apply to family members or close associates of such PEPs.

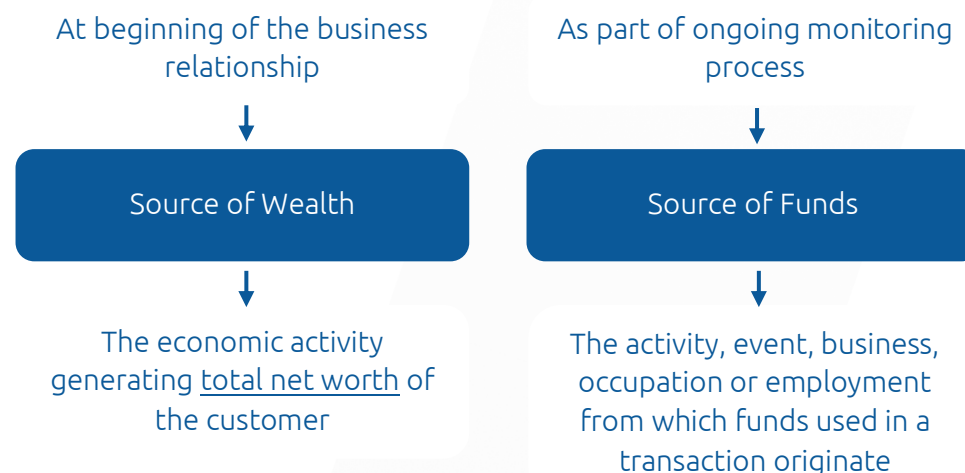
Source of Wealth and Funds

Establishing the customer's source of wealth (SoW) and source of funds (SoF) is a core requirement of EDD.

Source of Wealth refers to the origin of the customer's entire body of wealth (i.e. total assets). SoW explains activities the customer participates in and their geographical location. This information will usually give an indication as to the volume of wealth the customer could be expected to have, and a picture of how the customer acquired such wealth. When establishing SoW, there is no need to establish funds used in specific transaction. The goal of SoW establishment is to understand and verify, that customer's SoW corresponds with data given by the customer when onboarding and volume of the customer's wealth allows them to perform transactions with expected turnover specified by the customer.

Source of Funds refers to origin of funds being deposited, received, or transferred with the Company. SoF tells where the assets are coming from, which can be proven through bank statements, tax returns or the customer's financials, etc. Typically, SoW is requested when establishing business relationship or performing EDD, SoF is requested when there is a need to understand what the origin of a transaction is.

The types of data and documents that can be used for verification will vary depending on the circumstances and the information that the customer provides to the Company. The Company collects information relating to SoW or SoF of its customers and, according to the level of risk involved, takes reasonable steps to verify that information.



The following documents, data, or information could be considered reliable and independent:

- government-issued or registered documents or data;
- full bank and other investment statements;
- full pay slips or wage slips or other documents confirming salary;
- inheritance (stamped grant of probate, stamped grant of letters of administration);
- audited financial accounts from a chartered accountant or Charities Services;
- a copy of a will;
- sales and purchase agreements.

Ongoing Due Diligence

The Company must conduct ODD of business relationships and scrutinize the transactions undertaken throughout the course of that relationship to ensure that they are consistent with the Company's knowledge of the customer, the customer's economic activity and risk profile.

Ongoing monitoring of identity

In conducting ODD on the business relationship the Company has to:

- Ensure that documents, data and information collected under the CDD measures are kept up-to-date and relevant
 - obtain fresh documents when expiry date of identification documents held on file is reached;
 - question the data and information already in its possession whenever any inconsistencies arise;
 - obtain evidence of identity periodically to detect any changes;
 - refresh the data on key events (i.e. change of payment instrument).

The Company should determine on a risk-sensitive basis whether changes are substantial as to require re-assessment of customer risk of the business relationship.

Ongoing monitoring of transactions

Transaction monitoring is executed to prevent involvement of the Company with ML/FT/FP and to safeguard the reputation of the Company. While in conducting ongoing scrutiny of transactions the Company notices that the customer's transactions are not consistent with what it knows or expects from the customer, the Company has to question this unusual activity and, where necessary, establish the source of the funds used for that transaction. The reason for deviation may lie in inconsistency, amongst others, with the source of funds or average profile or account activity noted to date. The Company has to understand what the reason for this deviation is and obtain sufficient information and documentation with regard to the transaction. It is also one of the situations in which the risk profile of the customer may have to be revised.

After receiving the additional information the Company has to decide whether the transaction is an unusual transaction and need to be reported to the FIU.

Risk-based approach to monitoring

The extent of ongoing monitoring is linked to the determined customer's risk profile. The Company takes additional measures when monitoring the business relationships posing a higher risk. High-risk customers, for example PEPs, require more frequent and intensive monitoring.

The Company conducts ongoing monitoring on a risk-based approach and considers:

- the nature and type of transactions (e.g., abnormal size or frequency);
- the nature of a series of transactions (e.g., a number of transfers);
- the amount of any transactions, paying particular attention to particularly substantial transactions;
- the geographical origin/destination of a deposit or withdrawal;
- the customer's normal activity or turnover;
- specific transactions patterns, published by relevant authorities (e. g. FIU, FATF, CFATF).

The Company is vigilant for changes on the basis of the business relationship with the customer over time, which may include:

- new products or services that pose higher risk are entered into;
- new corporate or trust structures are created;
- the stated activity or turnover of the customer changes or increases;
- the nature of transactions changes or their volume or size increases etc.

Where the nature of the business relationship changes significantly, the Company carries out applies relevant measures to ensure that the ML/FT/FP risk involved, and nature of the business relationship are fully understood by the Company. Ongoing monitoring procedures take account the above changes.

Methods and procedures

When considering how to monitor its business relationship with the customer, the Company takes into account the following factors:

- the size and complexity of the Company's business;
- its assessment of the ML/FT/FP risks arising from the Company's business;
- the nature of the Company's systems and controls;
- the monitoring procedures that already exist to satisfy other business needs of the Company;
- the nature of the products and services (which includes the means of delivery or communication).

The Company takes the four steps systemic approach for ongoing monitoring of the business relationship:



Measures, used by the Company for ongoing monitoring of established business relationships is divided into two following categories.

Screening – monitoring transactions in real-time in real time on the basis of the parameters or characteristics previously determined. Screening measures are applied to the transaction before or immediately after completion of the transaction and may require the following actions:

- transaction suspension;
- application of EDD measures (incl. identification of SoF and the purpose of transaction);
- re-assessment of the customer's risk profile;

- sending an internal report to the Compliance Officer;
- sending an external report to the FIU.

Monitoring – analysis of transactions after their performance for the purpose to identify transactions and circumstances that could not be identified in real time or that, due to the nature of the transaction, did not appear in the parameters of screening. Monitoring measures may require the following actions:

- account suspension;
- application of EDD measures (incl. identification of SoF and the purpose of transaction);
- re-assessment of the customer's risk profile;
- sending an internal report to the Compliance Officer;
- sending an external report to the FIU.

In both cases (screening & monitoring), the Company uses technological solutions (incl. third-party solutions), as well as appoints employees responsible for the ongoing monitoring of the business relationships in according with requirements established.

Refusal or Termination of the Business Relationship

In case the obligations arising from the CDD application cannot be met, the Company cannot establish the business relation or perform the transaction or is obliged to terminate the business relationship with the customer. **The Company must keep a record of all the attempts made to get the necessary information and documentation.** To this end, the Company may decide to either close the account or to keep it blocked and suspended in its entirety. In the event that the customer makes the requested information and/or documentation available to the Company following the closure or the suspension and blocking of the account, the Company has to consider whether the delay in providing the requested CDD documentation and/or information affects the risk of ML/FT associated with the given business relationship.

The Company is to consider whether there are any grounds giving rise to suspicion of ML/FT/FP. The reluctance of the customer to provide CDD on its own should not be automatically equated to a suspicion of ML/FT/FP. The Company should consider all factors and information it has at his disposal to decide whether there are grounds to suspect ML/FT. **If however the presumption of ML/FT exist, the Company should submit an unusual**

transaction report to the FIU with regard to this customer. Where there is no reason for the retention of funds, the funds are to be remitted back to the customer. This has to be done through the same channels used to receive the funds.

Targeted Financial Sanctions

The Company takes measures to ensure compliance with the relevant regulations and legislation on sanctions in Curaçao. The Company takes into account at least the following sanction regimes:

- United Nations Security Council resolutions¹¹;
- Common Foreign and Security Policy of the European Union¹².

The Company shall monitor for amendments in Sanctions Decrees and Regulations on a regular basis, at least via the GCB website¹³, and update their CDD- and AML/CFT/CFP policies and procedures accordingly to reflect such amendments.

By the decision of the Compliance Officer, the Company may follow other sanction regimes and restrictive measures.

Procedure for identifying the subject of sanctions and a transaction violating sanctions

All customers should be screened against sanctions lists of the UN and EU. If Curaçao publishes a local list with designated persons and organizations, the Company should also take that local list into account. The Company must ensure it does not do business with customers that are subject to international sanctions. Before doing business or performing an occasional transaction for the first time with a customer, the Company should check published lists of known or suspected terrorists or other sanctioned persons or companies.

¹¹ <https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>

¹² <https://www.sanctionsmap.eu/#/main>

¹³ <https://www.gamingcontrolcuracao.org/notifications>

A mechanism must exist to check the sanction status of a withdrawing participant so that a sanctioned person or organization cannot remove money from an account that should be frozen.

Actions when identifying the sanctions subject or a transaction violating sanctions

Targeted financial sanctions require countries to freeze funds and assets and to ensure that no funds and other assets are made available, directly or indirectly, to or for the benefit of any designated persons or entities. The Company is required to freeze without delay and without prior notice, the funds or other assets of designated persons and entities taking into account the **process for the freezing of resources**¹⁴.

In a case the Company must apply a targeted financial sanction, **a report must be filed with the Curaçao FIU.**

Reporting Obligations

Recognition of Unusual Transactions

An unusual transaction is a transaction inconsistent with the customer's profile. Therefore, the first key to recognizing that a transaction or series of transactions is unusual is to know enough about the customer. The purpose of collecting information is to provide the Company with documentation to assess the risk that may be associated with the customer and to build a customer profile to assess how the customer is going to act within the framework of the business relationship.

In order to implement FATF recommendation 11, the Company must pay special attention to all complex, unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or visible lawful purpose. The following transactions or intended transactions shall be deemed unusual:

¹⁴ https://cbcs.spin-cdn.com/media/legislation_guidelines/20190120_process_for_the_freezing_of_resources_for_the_implementation_of.pdf

Objective indicators

The Company shall consider the following objective indicators:

- transactions which in connection with ML/FT/FP are reported to the Police or to the Department of Justice;
- transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- transactions in the amount of **NAf. 5,000 or more**, regardless of whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. A transaction may be a single transaction, but may also be a series, combination or pattern of transactions involving a total amount of the monetary equivalent of NAF. 5,000. This includes but is not limited to:
 - a cashless transaction in the amount of NAF. 5,000 or more. A cashless transaction is a transfer from a bank account of the Company to a local or international bank account, at the request of the customer;
 - accepting or releasing a deposit in the amount of NAF. 5,000 or more at the request of the customer;
 - sale to a customer of chips in the amount of NAF. 5,000 or more. "Chips" include but is not limited to tokens and credits;
 - a cash out in the amount of NAF. 5,000 or more.

Subjective indicators

The Company shall consider the following subjective indicators:

- transactions where there is cause to presume that they can be related to ML/FT/FP. Examples of situations that may be possibly related to ML/FT/FP include:
 - setting up dozens of betting accounts, with deposits well below reporting threshold to withdraw the money after a short while;
 - regularly depositing or transacting similar amounts of cash;
 - funding the account with credit and debit cards, prepaid cards, checks and cryptocurrency and then asking for a pay out;
 - unexplained income inconsistent with financial situation/customer profile;
 - customers claiming machine credits/payouts with no jackpot;
 - association with multiple accounts under multiple names;

- frequent betting transactions just under threshold;
- cash deposits/withdrawals just under threshold;
- parallel even money betting;
- betting against associates/intentional losses, where money launderers deliberately lose to one of the party who is able to receive a casino issued check or wire transfer of legitimate winnings (poker, roulette);
- multiple currency exchanges;
- currency exchange for no reasonable purpose;
- currency exchanges with low denomination bills for high denomination bills;
- currency exchanges with little or no gambling activity;
- wire transfers/currency exchanges just under thresholds;
- frequent 'cash out' transactions without corresponding 'buy in' transactions or vice versa;
- .

Reporting of Unusual Transactions

All unusual individual transactions or series of transactions must be reported internally to the Compliance Officer by filling approved **internal report in the form** (annex 5), **without any delay** but not later than the time periods specified in this section. All additional documents available, such as copies of identification documents, cash out slips, and other records must be also submitted as supplements.

The Company must report unusual transaction or any intended unusual transaction through the Compliance Officer to the FIU **without delay** but not later than the time periods specified in this section.

Reports of **objective indicators** must be submitted within **48 hours of transaction taking place**.

Reports of **subjective indicators**:

- Internal reporting to Compliance Officer to be submitted within **24 hours of transaction taking place**.
- The Compliance Officer has **10 working days** to complete relevant research.
- If presumption of ML/FT/FP exists, the compliance officer shall submit the report **within 48 hours** to the FIU.

A report shall contain, as far as possible, the following information:

- the identity of the customer;
- the nature and number of the client's identity document;
- the nature, time and place of the transaction;
- the size, destination and origin of the funds, securities, precious metals or other assets involved in the transaction;
- the circumstances on the basis of which the transaction is considered unusual.

The Compliance Officer must prepare a report of all unusual transactions for external reporting to the FIU according to the reporting regulations of the FIU. The Company shall report to the FIU the details of the transactions by means of the **goAML reporting portal**¹⁵. The reports and the submission of the thereto related information (all supporting documents) should be done in **English**. If internally reported transactions are not reported to the FIU, the reason shall be adequately documented and signed off by the Compliance Officer and/or senior management.

The Company and its directors, officers and employees are protected by law from criminal and civil liability for breach of any restriction on disclosure of information when reporting to the FIU.

Tipping Off

The Company and its senior management and employees shall not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU. They are not permitted to disclose information to the customer nor to third parties. The reason for this is not to jeopardize an analysis or investigation into ML/FT/FP. Caution is advised when the Company takes action to terminate a relationship or otherwise block additional transactions following reporting to the FIU. Drastic action should only be taken when there is no other way out, since any unjustified action may alert the customer. In such circumstances, it would be more advisable to increase on-going monitoring and submit additional reports to the FIU on any other suspected instances of ML/FT/FP.

¹⁵ https://portal.fiucuracao.cw/goAMLWeb_PRD/Home

Record keeping

The Company shall record the following data in such a way that it is accessible:

- the name, address and domicile or place of business of the customer and, if any, the ultimate beneficial owner and of the person in whose name the deposit or account is made, of the person who will have access to the safe deposit box or the person in whose name a payment or transaction is made, as well as their representatives;
- the nature, number, date and place of issue of the document by means of which the identity was established;
- the nature of the service; and
- the nature, origin, destination, extent and other unique characteristics of the values or items concerned in a transaction.

The Company shall maintain, **data referred to above as well as all other relevant data relating to both domestic and international transactions** for at least **5 years after the execution of the transactions** in question, in such a way that those data are retrievable and the transactions in question can be reconstructed for a period of **5 years** to enable them to comply with information requests from the competent authorities. The Compliance Officer shall adequately document unusual transactions. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

The FIU or a staff of the FIU to be designated by the FIU, may, in the case of a transaction that has been reported to the authorities, charged with the investigation and prosecution of criminal offences, issue an instruction to set the retention period at **10 years**. Acting contrary to such instruction is prohibited.

The Company shall keep **data and documents obtained through the CDD measures application**, including the risk profile of the customer, contact information and the copies or registers of official identity documents and passports, identity cards, driving licenses or similar documents, account statements and business correspondence, in an accessible manner **for at least 5 years after the termination of the business relationship**.

The data and information obtained from the CDD and transaction files shall be made available without delay to the competent authorities and the authorities that are authorized to inspect or obtain this information on the basis of the NOIS.

The CDD information and the transaction records should be available to domestic competent authorities based upon appropriate legal authority.

Training and Screening of Employees

The Company shall screen their employees for criminal records before the conclusion of employment contract.

The Company shall develop training programs and provide training to its employees. Training includes setting out rules of conduct governing employee's behavior and their ongoing education to create awareness of the Company's AML/CFT/CFP systems and procedures. Most areas of the Company should receive training, and the target audience should include most employees. However, each segment should be trained on topics and issues that are relevant to them. Training must at least address the following topics in regard to different types of employees:

For new KYC Agents (i.e. employees who will handle customers or their transactions), irrespective of their level of seniority:

- the nature and process of ML, FT and FP;
- the Company's existing internal policies, procedures concerning ML, FT and FP;
- regulations concerning ML, FT and FP;
- the reporting requirements;
 - the need to report any unusual transactions to the appropriate designated officer;
 - objective and subjective indicators for reporting unusual transactions;
- ML methods and trends in the gambling sector;
- explanation on CDD.

For audit staff:

- the Company's existing internal policies, procedures concerning ML, FT and PF;
- regulations concerning ML, FT and PF;
- ML methods and enforcement, and their impact on the Company.

For Compliance Department staff:

- the Company's existing internal policies, procedures concerning ML, FT and PF;
- regulations concerning ML, FT and PF;
- ML methods and trends in the gambling sector;
- ML methods and enforcement, and their impact on the Company.

For supervisors and managers:

- a higher-level instruction of the Company's existing internal policies, procedures concerning ML, FT and PF;
- a higher-level instruction of the regulations concerning ML, FT and PF.

For senior management and board of directors:

- ML methods and trends in the gambling sector;
- ML methods and enforcement, and their impact on the Company.

The training held is to be documented and confirmed with the employees' signatures on the **training protocol** (annex 6). This protocol should include:

- details on the content of the training programs;
- the names of the staff members who have received the training;
- the date on which the training was provided;

To demonstrate compliance with the abovementioned training guidelines, the Company shall also maintain records that include:

- the results of any testing carried out to measure staff understanding of ML, FT and FP requirements; and
- an ongoing training plan.

Refreshment training must be arranged at regular intervals to ensure that staff members are kept informed of current and new developments regarding ML, FT and FP techniques, methods and trends.

Independent Audit of the AML/CFT/CFP Policy

The AML/CFT/CFP Policy must be monitored and evaluated **at least annually** by an adequately resourced internal audit department or an outside independent party (hereinafter – Internal Auditor). The audit must be independent, thus performed by Internal Auditor not involved with the organization's AML compliance staff (incl. the KYC Agents and the Compliance Department). Internal Auditor performing the audit must be sufficiently qualified to ensure that their findings and conclusions are reliable. These tests must include at least:

- an evaluation of the institution's AML, CFT and CFP manuals;
- customer's file review;
- compliance management;
- performance of transaction testing;
- assessment of training adequacy;
- assessment of compliance with applicable laws and regulations;
- evaluation of the system's ability to identify unusual activity;
- interviews with employees who handle transactions and with their supervisors;
- a sampling of unusual transactions on and beyond the threshold(s) followed by a review of compliance with the internal and external policies and reporting requirements; and
- an assessment of the adequacy of the record retention system.

The Internal Auditor should also consider whether the Company's senior management and board of directors were responsive to earlier audit findings.

The scope of the testing and the testing results must be documented within the **internal audit report form** (annex 7), with any deficiencies reported to senior management and/or the board of directors, and to the designated officers with a request to take prompt corrective actions by a certain

deadline. These corrective actions could also include enhancement of controls and procedures. The provided internal control report shall include at least the following:

- period of exercising the internal control;
- name of the person executing the internal control;
- description of the internal control measures that has been performed;
- results of the internal control;
- determined deficiencies, which were eliminated in the period of exercising the internal control;
- determined deficiencies, which were not eliminated at the end of period of exercising the internal control;
- measures that are required to implement for elimination of determined deficiencies;
- general conclusions from the exercised internal control.

The senior management and/or the board of directors shall review the internal control report provided and make resolution regarding it. The Internal Auditor shall be notified about the essence of such resolution in format which can be reproduced in writing. For this reason, the senior management and/or the board of directors is obliged to:

- analyze the results of performed internal control;
- implement actions to eliminate deficiencies occurred.

Examination by the Gaming Control Board

The Company shall provide information or documentation on their ML, FT and FP and deterrence and detection procedures to the examiners of the GCB in preparation of or during an examination and upon GCB request during the year. The Company shall make the following items readily available:

- its written and approved AML/CFT/CFP Policy on ML, FT and FP;
- records of its Business Risk assessment;

- the name of each Compliance Officer responsible for the Company's overall ML, FT and FP policies and procedures and his/her designated job description;
- records of reported unusual transactions;
- records of unusual transactions which required closer investigations;
- records of frozen accounts;
- schedule of the training provided to the Company's personnel regarding ML, FT and FP;
- the assessment report on the Company's policies and procedures on ML, FT and FP by the internal audit department or an external auditor;
- the customer's files including customer risk assessment, CDD, customer acceptance and transaction information.

Annexes

Annex title	Document description
1. Resolution of approving the AMLCFT Policy	The Company's senior management's and/or the board of directors' draft for approving this AML/CFT/CFP Policy.
2. Decision for the Compliance Officer Appointment	The Company's senior management's and/or the board of directors' draft for the appointment of Compliance Officer.
3. List of Risk Factors	List of risk factors which are used for determination of the Customer's risk profile.
4. Internal Report Form	Internal reporting form which should be filled by the KYC Agent when notifying the Compliance Officer
5. Training Protocol	Form which should be signed if the employee has passed the relevant training.
6. Internal Audit Report Form	Report form which should be filled and provided by the Internal Auditor to the senior management and/or the board of directors.
7. Competent Authorities' Guidelines	Guidelines of FIU, FATF and CFATF which are related to the Company's activity.



Version Control Table

Approval date	Changes description
21.05.2025	First issue

Resolution

Name of the company: Aquarius Entertainment N.V.

Reg. number: 161153

Registered office of the company: ~~Abraham de Veerstraat 9 Curacao~~
Schottegatweg Oost 10, Bon Bini Business Center
Unit 1-9, Willemstad, Curaçao

The manager of the company hereby decides:

Accept and approve the AML/CTF Policy (incl. its annexes), which was developed and reviewed on 21.05.2026

DocuSigned by:

BFFB053659204B9...

Kurason Trust Curaçao N.V.

By: Jonathan Heymans

Managing director


Sarunas Masalas
Compliance Officer

Decision

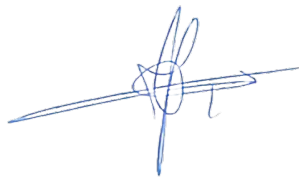
Name of the company: Aquarius Entertainment N.V.

Reg. number: 161153

Registered office of the company: Schottegatweg Oost 10, Bon Bini Business Center
Unit 1-9, Willemstad, Curaçao

The Senior Management of the company hereby decides:

Appoint Sarunas Masalas (DOB: 17.11.1987) as the as the Compliance Officer responsible for the detection and deterrence of ML/TF.



Kurason Trust Curaçao N.V.

By: Jonathan Heymans

Managing director

Business Risk Assessment Report

Aquarius Entertainment N.V.

Curaçao

May 2026

Approval date	Board of directors' signature
21.05.2026	

Table of Contents

Table of Contents	2
Purpose	3
Sources used	3
Understanding the Company's Business.....	3
Methodology	4
Risk identification	4
Risk analysis and evaluation	5
Inherent risk assessment	5
Mitigation measures assessment.....	7
Residual risk assessment	8
Risk appetite	9
Annexes	10

Purpose

This Business Risk Assessment Report ("BRA") identifies, assesses, and documents the ML/FT/FP risks arising from the Company's operations as an online casino in Curacao, establishing the grounds and principles for the Company's ML/FT/FP risk management framework.

The purpose of the BRA is to:

- identify inherent ML/FT/FP risks associated with the Company's business operations;
- evaluate the likelihood and impact of those risks;
- assess the effectiveness of mitigating controls;
- determine the Company's residual risk exposure; and
- support compliance with applicable AML/CFT/CFP obligations.

Sources used

The BRA has been prepared using the following sources:

- internal AML/CFT/CFP policies and procedures;
- the latest national risk assessment on ML of Curaçao;
- FATF and similar international organizations' guidance and typology reports applicable to online casino operators;
- national AML/CFT/CFP regulations and regulatory guidance applicable to online casino operators, primarily;
- other industry guidance for online casino operators.

Understanding the Company's Business

The Company operates an online casino platform offering remote gambling services to customers across various jurisdictions. The fully remote and cross-border nature of the business increases exposure to financial crime risks, particularly in relation to customer onboarding and source/destination of funds verification.

Key elements of the Company's business operations which are considered in the risk assessment include:

- business relationship establishment;
 - the Company establishes business relationships remotely;
 - the Company establishes business relationships only with natural persons;
 - the Company accepts customers from various countries (incl. countries in high-risk lists);
- deposits and withdrawals;
 - the Company allows to make deposits and withdrawals for the use of the services using both fiat currencies and crypto assets;
 - the payment processing is done through third-party providers;
- casino gameplay and wagering;
 - the Company provides its services via its online platform;
 - the estimated average amount of a single transaction ranges from 1.5-1,000 USD;

- the estimated average monthly deposit amount is 10,000 USD.
- customer relationships management;
 - the Company communicates with the customers via email.

By detailing the services or products offered, how and where they are provided, the Company is able to assess risks effectively. It ensures compliance with applicable regulations, addresses potential ML/FT/FP risks and outlines how resources will be allocated to manage these risks. Additionally, it provides a basis for continuous monitoring and quick adaptation to emerging threats, helping the Company stay resilient in the face of challenges.

Methodology

When conducting the BRA, the Company follows the risk assessment process detailed in the Company's AML/CFT/CFP Policy, consisting of the following stages:

- risk factors identification;
- risks factors analysis;
- risks factors evaluation.

Risk identification

This process consists of the identification and description of events that threaten the achievement of the Company's objectives (risks). It also seeks to identify the risks arising from missed opportunities and the opportunities arising from addressing risks.

To identify risks, the Company is guided by the following objectives:

- what could go wrong (event)?
- why might something go wrong (risk factors, i.e. causes)?
- what are the possible consequences (impact)?

When identifying risks, it must be taken into account that different risk factors may lead to the same risk materializing, the same risk factor may lead to different risks materializing and a risk may have multiple adverse consequences. The Company determines if there are any requirements for managing specific risks and develop description of such risks according to such requirements, as well as decides if there's any risks which the Company intends to manage according to business decision (i.e. without an obligation arising from applicable legislation or other sources).

The Company categorizes the risks across the following key categories:

- **customer risk** - the risk for the Company to be potentially abused due to the business field or profile of the customer or the acts of customer or those acting on behalf or for the benefit of the customer for money laundering or terrorist financing purposes;
- **geographic risk** – the risk of potential financial, legal, or reputational losses that may arise from operating in a foreign country and exposing itself to unfamiliar regulations, a different legal system, and potentially unstable political environments;
- **service risk** - the potential risk that products or services offered by the customer may be misused by the criminals for money laundering or terrorist financing activities;

- **delivery channel risk** – the risk of potential misuse of the financial channel supplied through the customer for ML/FT/FP.

The Company has described the risks identified in a reasonably generalized formulation in the **Risk Register** (annex 1).

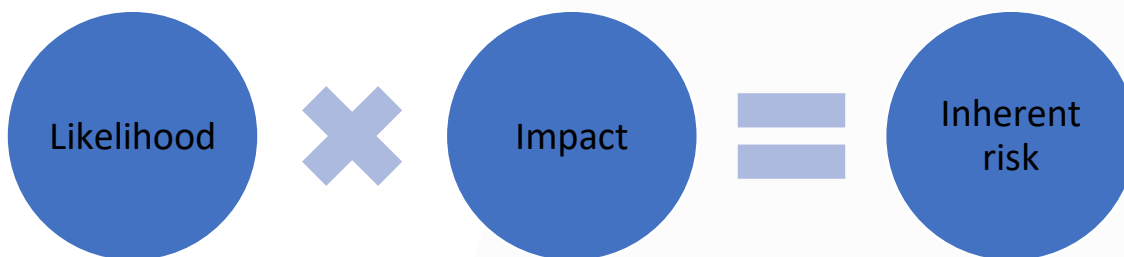
Risk analysis and evaluation

In the course of this process the Company identifies possible consequences (impact types) arising from risks to be managed, methods (incl. scales) for risks assessment and maximum acceptable value of such consequences. Each risk factor is assessed based on:

- likelihood of misuse for ML/FT/FP purposes;
- potential regulatory, legal, financial, and reputational impact;
- complexity and scale of exposure;
- availability and effectiveness of mitigating controls.

Inherent risk assessment

Inherent risk level is found via an assessment of the risk factors using the following formula:



Likelihood is the probability that a given risk event will occur, which can be expressed using numerical values (1-4), as a score to measure the probability, complexity of a business process and frequency. Likelihood is found using the following criteria against three separate dimensions:

Likelihood of a risk event			
Score	Possibility	Complexity of a business process	Frequency
4	More often than once a year	Business is very complex; changes in the business process are significant and frequent.	The risk occurred within the last year and mitigation measures have not yet been implemented.
3	Once a year	Process of above average complexity.	Risk has occurred in the last 3 years and mitigation measures have not yet been implemented.

2	Once during three years	Process of medium complexity.	The risk has not yet materialized and may occur in very specific circumstances.
1	More rarely	The process is simple, straightforward and stable, with few participants.	The risk has not yet materialized; The risk has occurred in the past, but adequate mitigation measures were applied to reduce the likelihood of the risk occurring.

The score should be assigned, if at least one Likelihood with such score exists regarding risk factor (e.g., if possibility is 4 and all others are 1, for example, then the overall Likelihood = 4).

Impact is the extent to which a risk event might affect the Company, which can be expressed using numerical values (1-4), as a score to measure the impact on four separate dimensions (financial, reputational, business interruption, legal). Impact is found using the following criteria against four separate dimensions:

Impact of a risk event				
Score	Financial impact	Reputational impact	Business interruption	Legal impact
4	Decrease in revenue or increase in costs >20%;	Reputational impact significant and long-lasting, negative news in national publications, social media coverage, as well as international mentions.	Long-term business process interruption. Significant negative impact on the Company's objectives.	License revocation; Significantly material penalty; Loss of critically important outsourcing partner.
3	Decrease in revenue or increase in costs 5%-20%;	Reputational impact Significant and short-lived, negative news in a national publication, social media coverage.	Business process interruption can be restored in a longer time than planned	Monetary Penalty
2	Decrease in revenue or increase in costs 2%-5%;	Reputational impact short term and insignificant	The business process breaks down, but quickly recovers	Regulatory precept
1	Decrease in revenue or increase in costs <2%;	No reputational impact.	Business process is not interrupted, but there are glitches	No legal impact

The score should be assigned, if at least one impact with such score exists regarding risk factor (e.g., if financial impact is 4 and all others are 1, for example, then the overall Impact = 4).

4	8	12	16
3	6	9	12
2	4	6	8
1	2	3	4

According to the assessed likelihood and impact level, the risk is assigned a corresponding **Risk Level**:

- Red - Critical
- Orange - High
- Yellow – Medium
- Green – Low

The Company evaluates each risk factor to determine the inherent risk score which is specified in the **Risk Register**.

Mitigation measures assessment

After the inherent risk has been identified, the Company performs an assessment of the **mitigating measures** and controls to evaluate the appropriateness and effectiveness of such measures. The following scale should be used for evaluation of mitigating measures.

Mitigation Measure Effectiveness	Description of the effectiveness of the mitigation measure
Effective (score - 4)	Systems and processes effectively mitigate risk, accountability is clear, well documented, and subject to regular and appropriate monitoring. There is a high level of confidence that the risk is avoided or mitigated properly.
Sufficient (score - 3)	Mitigation measures contribute to reducing risk. Process improvements are needed to achieve better efficiency. There is reasonable assurance that the risk is avoided or mitigated properly.
Insufficient (score - 2)	Mitigation measures have a limited impact on risk mitigation, and processes and systems need significant improvement and monitoring. There is insufficient assurance that the risk is avoided or mitigated properly.
Not acceptable (score - 1)	Mitigation measures do little or nothing to reduce the impact of inherent risk. Immediate management intervention and efforts are necessary to manage the risk. Significant re-design and streamlining of processes and systems required. There is a belief that the risk can't be avoided or mitigated properly.

Factor-specific mitigation measures and the evaluation results are placed into the **Risk Register**. In addition to the factor-specific measures, the Company also considers the following generally applicable ML/FT/FP risk mitigation measures applied by the Company, including:

- preparation and the regular review of an AML/CFT/CFP Policy;
- regular internal audit of the effectiveness and compliance with the AML/CFT/CFP Policy;
- defining the responsibilities of relevant persons under the AML/CFT/CFP Policy (incl. appointment of a qualified Compliance Officer);
- establishment and application of CDD/EDD/ODD procedures;
- establishment of internal unusual transaction reporting channel(s) and the obligation to report unusual transactions or the suspicion thereof (incl. external reporting);
- screening and periodic AML/CFT/CFP training of employees;
- establishing the consequences of violations of the obligations under the AML/CFT/CFP Policy.

Residual risk assessment

After inherent risks and controls have been evaluated, the Company calculates residual risk score for each risk factor and puts the results to the **Risk Register**.

Residual Risk is assessed using the following formula:



The Company should also calculate average residual risk score for each risk and risk category (if any).

According to the assessed inherent risks and controls, the score of residual risk shall be determined as follows:

Effectiveness of Migration Measures					
Inherent Risk	Score	Effective	Sufficient	Insufficient	Not acceptable
	Critical	Low	Medium	High	Critical
	High	Low	Medium	High	High
	Medium	Low	Low	Medium	Medium
	Low	Low	Low	Low	Low

As result of the above process, the Company analyzes if there is a necessity to implement any of the following actions:

- amending and approval of the Company's Risk Appetite;

- implementation of additional mitigating measures;
- ongoing continuous monitoring (incl. enhanced monitoring);
- making changes in business process(es).

Risk appetite

As result of the above process, the Company establishes its risk appetite, which is outlined in the **Risk Appetite statement** (annex 2).

Annexes

Annex title	Document description
1. Risk Register	Documentation of the identified ML/FT/FP risks and their assessment.
2. Risk Appetite Statement	The articulation in written form of the aggregate level and types of risk that the Company is willing to accept, or to avoid, in order to achieve its business objectives.

Risk Appetite Statement

Aquarius Entertainment N.V.

Curaçao

May 2026

Version Control Table

Approval date	Changes description	Board of directors' signature
21.05.2026	First issue	

Introduction

The Company's Risk Appetite Statement articulates the Company's philosophy and approach to the management of its key ML/FT/FP risks based on the business risk assessment (BRA) carried out as well as guides decision-making and ensures appropriate governance around risk-taking within the Company.

The Company's Risk Appetite is the type and the amount of risk that the Company is willing to accept or to avoid in order to achieve its business objectives. The Risk Appetite Statements clarify those risks and associated limits that the Company must manage and, where appropriate, is prepared to accept in the pursuit of its vision and objectives.

The Senior Management is responsible for setting the Risk Appetite of the Company which it reviews and approves **at least annually**. The Senior Management of the Company is responsible for ensuring that their business is operating within their stated Risk Appetite parameters. The Company's Risk Appetite is forward-looking and it evolves to reflect external market developments and the Company's strategic focus.

Risk Appetite Statement

The Company has a **medium-to-high** risk tolerance for ML/FT/FP risk. This includes undertaking activities that may involve elevated inherent or residual risk, provided such risks are identified, assessed, and considered controllable to a large extent through appropriate governance, oversight, and risk mitigation measures. The Company does not seek to eliminate all risk but aims to manage it responsibly to support sustainable growth and informed decision-making.

At the same time, the Company maintains a zero-tolerance approach toward ML/FT/FP, sanctions violations, and other illicit use of its services. To mitigate these risks, the Company implements proportionate mitigation measure and controls within its AML/CFT/CFP Policy to identify, investigate, and report suspicious or unusual activities and to prevent misuse of its services for unlawful purposes.

The established ML/FT/FP risk management controls are proportionate to the risks faced by the Company. The Company is committed to combating financial crime and continually strives to ensure that accounts held at the Company are not misused for the purpose of ML/FT/FP. In line with this, the Company will not:

- knowingly facilitate criminal activities carried out by customers;
- accept any deliberate or systemic breaches of applicable laws and regulations;
- facilitate transactions with individuals that cannot be identified in accordance with Company's AML/CFT/CFP Policy and are unresponsive to information requests by the Company which is significant to their identification, or intentionally provide misleading information to the Company which is significant to their identification or activities;
- allow the use of the Company's services using anonymity-enhancing methods, including:
 - use of certain crypto assets, accounts/wallets and payment institutions/VASPs;
 - use of measures which allow to conceal the location of the customer's devices;
 - use of un-approved identification and communication methods;
- establish or continue business relationships with customer who are subject to risk factor(s) with prohibited risk in accordance with the Company's **List of Risk Factors**, including:
 - customers with certain characteristics (incl. behavior, area of activity, age restrictions);

- customers residing in certain countries;
- the manner in which customers use or request to use the Company's services.

This approach allows the Company to onboard and service a wider range of customers, including those presenting elevated inherent risk, where such relationships are lawful and commercially justified. Customers subject to low-high risk factors determined in the **List of Risk Factors** may be accepted by the Company. Customers subject to one or more high risk factors (as determined by the Company's customer risk assessment) must be subjected to the relevant EDD measures in accordance with the AML/CFT/CFP Policy prior to onboarding and on an ongoing basis.

List of Risk Factors

Aquarius Entertainment N.V.

Curaçao

May 2026

This List of Risk Factors (List) establishes the risk factors and their risk levels which the Company uses in the course of CDD measures application, as described in the AML/CTF Policy which annex this List is, to establish the presence of the relevant risk factor in relation the customer which may affect the risk of ML, FT, FP or violation of Sanctions within the course of services provision.

The Company does not enter into the Business Relationship with customers regarding whom the presence of a risk factor with risk level “prohibited” is established as identified in the table below.

The Company assesses the following risk factors.

Risk level	Risk category	Risk factor
Low-Risk	Risks related to customers	The customer has a single source of regular income
	Risks relating to communication, mediation of products, services, transactions or delivery channels between the Company and the Clients	- The customer makes payments within the scope of the business relationship only via an account located in a credit institution whose place of business is in EEA - The customer is identified on a non-face-to-face basis using technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations.
Medium-Risk		There are no risk factors identified in regard to the customer
High-Risk	Risks related to customers	The customer’s economic activity includes one of the following activities: private or personal banking, providing or intermediating a product or service which may promote anonymity, personal asset holding, undertaking handling large amounts of cash, currency exchange, conversion transactions, providing gambling services (in a casino, on the internet or at sports events etc.), purchasing and selling gold (incl. scrap gold), other precious metals or gemstone, purchasing and selling luxury goods, providing internet advertising, providing innovative services, extractive

		industry, non-governmental organization, providing adult entertainment services, legally purchasing and selling marijuana, virtual assets related business, regulated charity, embassy/consulate. • The customer is subject to negative news related to ML, FT, FP, violation of Sanctions and/or other offences (Adverse Media) • The customer has provided incomplete or insufficient KYC information • The customer's appearance and behavior are not in line with the nature of the transaction performed by the customer • The customer is significantly old (age over 70) • The customer is a PEP • The customer has a known connection to a PEP (the family member of the PEP or a close associate of the PEP) • The transactions or activity of the customer does not correspond with its declared activity, financial profile, transactional profile or its background • The customer is lacking knowledge or providing inaccurate information about the transaction, the source of funds (incl. providing information indicating that the transaction is in support of illicit activities) • The customer's identification or account credentials (e.g. a non-standard IP address, or flash cookies) are shared by another account
	Risks relating to countries, geographic areas or jurisdictions	• The customer's place of residence or location is in a country which is on the FATF list of Jurisdictions under Increased Monitoring¹ • The customer's place of residence or location is in a country which is on the European Commission's list of third countries having strategic deficiencies in their AML/CFT regime² • The customer's place of residence or location is in a country which is identified as Jurisdictions of Concern or Primary Concern in the U.S. Department of State's annual International Narcotics Control Strategy Report³. • The customer's place of residence or location is in a country or jurisdiction, which according to credible sources, has significant levels of corruption (CPI <30) or other criminal activity (crime index >60)⁴ • The customer's place of residence or location is in a country which is on the CFATF Public Statement⁵
	Risks relating to products, services or transactions;	• The customer's activity suggests that the customer might favor anonymity (e.g. use of virtual assets or pre-paid cards in transactions). • The customer holds numerous accounts or wallets with the Company.

¹ <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>

² <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R1675-20230316%20>

³ <https://www.state.gov/international-narcotics-control-strategy-reports/>

⁴ <https://www.transparency.org/en/cpi/2020/index/nzl>

https://www.numbeo.com/crime/rankings_by_country.jsp

⁵ <https://www.cfatf-gafic.org/home/public-statements>

	Risks relating to communication, mediation of products, services, transactions or delivery channels between the Company and the customers	• The customer is identified on a non-face-to-face basis NOT using technological measures and controls to address the heightened risk of identity fraud or impersonation present in these situations. • The customer's IP address or location differs from used in the course of onboarding and there's no logical explanation
Prohibited	Risks related to customers	• The customer is under the age of 18 or the legal age at which gambling, or gaming activities are allowed under the law or jurisdiction that applies to the customer • The customer is a legal entity or another association of persons not having the status of a legal entity. • The beneficial owner of the customer is some third person. • The customer is a subject of EU, UN or OFAC sanctions. • The customer is an employee/officer or any key person of the Company or any person who is a UBO or any employee/officer of any entity which has a qualifying interest. • The customer has excluded themselves from participation and the self-exclusion period is in place. • The customer does not facilitate compliance with the relevant CDD measures. • The customer has provided forged or edited KYC documents (e.g., identity documents, source of funds, etc.). • The customer is a section 311 designated entity⁶. • The customer's economic activity includes one of the following activities: purchasing and selling arms or atomic power, unregulated charity.
	Risks relating to countries, geographic areas or jurisdictions	• The customer's place of residence, establishment or location is in the EEA • The customer's place of residence or location is in a country which is subject to sanctions, embargos or similar measures issued by the EU, UN or OFAC⁷ • The customer's place of residence or location is in a country which is on the FATF list of High - Risk Jurisdictions subject to a Call for Action⁸. • The customer's place of residence or location is in a country which is included in the list of the State Sponsors of Terrorism⁹

⁶ <https://www.fincen.gov/resources/statutes-and-regulations/311-and-9714-special-measures>

⁷ <https://www.sanctionsmap.eu/#/main>

<https://www.un.org/securitycouncil/sanctions/information>

<https://sanctionssearch.ofac.treas.gov>

⁸ <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>

⁹ <https://www.state.gov/state-sponsors-of-terrorism/>

		The customer's place of residence or location is in Curaçao, or any other territory as determined by the GCA from time to time, including: Australia, France, Netherlands, USA, Dutch Caribbean territories (Aruba, Bonaire, Curaçao, St. Maarten, Saba, and St. Eustatius).
	Risks relating to products, services or transactions;	- The customer is providing fraudulent documents in the course of service provision (incl. SoW/SoF documents, etc.). - The customer requests to use settlement channels and accounts belonging to unknown or unrelated third persons. - The customer requests to open an anonymous or fictitious named account.
	Risks relating to communication, mediation of products, services, transactions or delivery channels between the Company and the customers	- The customer uses an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs. - The customer is using TOR when requesting the services - The customer uses credit institution, financial institution, paying institution, e-wallet or payment channel that promotes anonymity (incl. shell banks) or that is in a high-risk country. - The customer's IP address or location in the course of onboarding is related to the following countries or jurisdictions, which provide funding or support for terrorist activities: Cuba, Iran, North Korea, Syria.

Internal Report

This establishes the form of report that the employee must fill in and forward to the Compliance Officer in cases specified in AML/CTF Policy.

Employee Details

Name of the employee
sending report:

Customer's Details

The customer's name:
Personal identification
code or date of birth:

Transaction Details

Transaction amount:

Transaction time:

Transaction
description:

Additional Information and Grounds for Doubt

The Compliance Officer Resolution and Performed Activities

Notification arrival date:

Performed actions:

Date of notification to the
competent authority:

Brief description of the
notification to the
competent authority:

List of Attachments:

- 1.

Training Protocol

Content of the training	
Date of the training	

List of participants

	First and last name of the participant	Signature
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		

Internal Audit Report

Internal Control Officer name:	
Reporting period:	

Description of the internal control measures that have been performed

Results of the internal control

Determined deficiencies, which were eliminated in the period of exercising the internal control

Determined deficiencies, which were not eliminated at the end of period of exercising the internal control

Measures that are required to implement for elimination of determined deficiencies

General conclusions from the exercised internal control

The AML/CFT/CFP Regulations

Applicable for Curaçao casinos and providers of other online games



G. Schorea / J. Leppers

July 8, 2024



GCB

Curaçao Gaming Control Board

“ELEVATING THE CURAÇAO GAMING INDUSTRY”

Table of Contents

1. *Introduction*
2. *The Risk-based Approach*
3. *Customer Due Diligence*
 - *Standard Customer Due Diligence*
 - *Enhanced Due Diligence*
 - *Simplified Due Diligence*
4. *Reporting of unusual transactions*
5. *AML Compliance Program*
6. *Record keeping requirements*
7. *Questions*



Introduction

Rec
22

R10 - CDD

R11 – Record Keeping

R12 – PEP

R15 – New Technologies

R17 – Reliance on Third Parties

DNFBPs

Rec
23

R18 – Internal Controls

R19 – Higher Risk Countries

R20 – SAR Reporting

R21 – Tipping Off & Confidentiality

Introduction

Measures to mitigate ML/FT/FP Risk

- The measures, policies, controls and procedures to mitigate ML/TF risk are to include:
 - **CDD**
 - **Record keeping procedures**
 - **Reporting procedures**
 - **Risk management measures** including customer acceptance policies (CAP), CRA procedures, internal control, compliance management, training and employee screening policies and procedures

Risk-based approach

FATF Recommendations require a risk-based approach ('RBA') as to combat of ML/TF: preventive measures must be commensurate to risk identified.

Thus: enhanced or simplified measures, depending on risk.

RBA:

- Assessment of ML/TF risk
- Risk mitigating policies, procedures and controls
- Monitoring and improving effective operations of the above
- Documentation of ML/TF risk assessments



Risk factors:

- Player
- Country
- Product
- Service
- Delivery channels

Consideration of National Risk Assessment

Risk assessment to be submitted to GCB upon request

Risk assessment:

- Business risk assessment (BRA)
- Customer risk assessment (CRA)

BRA:

How can my products and services be used for ML/TF?

What is my risk appetite?

-> AML/CFT compliance program

Requirements of BRA:

- Revision in case of environmental changes or changes within business activities
- Annual revision in case of no changes
- Documentation of:
 - methodology
 - reasoning for L/M/H risk rating
 - outcome BRA
 - sources of information used
- Approval by Board of Directors

CRA:

What ML/TF risks am I exposed to with this player?

- > Customer Due Diligence (CDD)
- > Customer Acceptance Policy (CAP)

CAP content:

- Description of players posing higher risk
- Risk indicators (L/M/H)
- Level of CDD to be applied (inclusive of ongoing monitoring)

Considerations:

- Politically exposed persons (PEPs)
- Sanctions screening

AML/CFT policies, procedures and controls should cover:

- CDD
- Record keeping procedures
- Reporting procedures
- Risk management (CAP, CRA)

Table 5 – Risk-scoring grid

	Scoring	Type of Customer	Product/Service	Interface	Geographical Connections
VERY HIGH	9-10	• Unregulated virtual currency exchanges • Corporate structures involving the use of bearer shares	• Services intended to render the customer anonymous	• Non-face to face through intermediaries	• Country subject to sanctions, embargoes
HIGH	6-8	• Non-Profit Organisations sending funds to non-reputable/high-risk jurisdictions • Correspondent banks • Fiduciary arrangements	• Internet-based products • Services or products identified as posing a high risk of ML/FT	• Non-face to face using means with no embedded technological safeguards	• Non-reputable/high-risk jurisdiction
MEDIUM	3-5	• Highly paid employees • Public figures • General public	• Retail products	• Non-face to face (using technological systems with embedded safeguards)	• Reputable jurisdiction
LOW	1-2	• Other individuals (e.g., pensioners, average-salaried employees)	• Products with very limited transaction/deposit thresholds	• Face to face	• EU Member State • Domestic

Customer Due Diligence

- A sound CDD program is the best way to prevent ML/TF
- CDD should provide confidence that you know your customer and that your service or product is not being used as a tool to launder money or any other criminal activity
- The casino operator is prohibited from keeping anonymous accounts or accounts in obviously fictitious names

Customer Due Diligence

- The casino operator has to undertake CDD measures when:
 - Players engage in financial transactions $\geq$ NAf. 4,000
 - Carrying out occasional transactions > the monetary equivalent of NAf. 4,000 (or a series of two or more related transactions)
 - There is a suspicion of ML or TF
 - The casino operator has doubts about the veracity or adequacy of previously obtained customer identification data

Customer Due Diligence

- The CDD measures to be taken are as follows:
 - Identifying the customer and verifying customer's identity
 - Identifying the beneficial owner, and taking reasonable measures to verify the identity of the Beneficial owner
 - Understanding and obtaining information on the purpose and intended nature of the business relationship
 - Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure transactions are consistent with institution's knowledge of customer, business risk profile, including, where necessary, the source of funds

Customer Due Diligence

- Timing of CDD measures implies that:
 - CDD measures (1-3) must have been completed at time Naf. 4,000 threshold is reached
 - Casinos required to apply minimum level of CDD measures when entering business relation (opening account)
 - At least personal details to be collected and sanctions screening to be conducted when opening account
 - Players may be allowed to use their gaming account while carrying out CDD measures

Customer Due Diligence

- However, if Naf. 4,000 is reached → players are not allowed to deposit funds to or withdraw funds from the account
- Threshold to be calculated on a daily basis taking all deposits and withdrawals into account since establishment of business relationship including peer-to-peer transfers
- If documentation not received within 30 days the threshold is reached → casino must terminate business relationship and report transaction to the FIU if presumption of ML exists
- Carrying CDD at the earliest possible can limit situations in which ill-gotten funds are received

Identification and verification

The personal information to be collected and the extent of verification to be carried out, is to be determined on the basis of risk

1. Identification of the player

- Identification is the collection of a series of personal details on the customer. The standard procedure consist of gathering following details:
 - Name and surname
 - Permanent residential address
 - Date of birth
 - Place of birth
 - Nationality
 - Identity number

Identification and verification

2. Sanctions screening

- Sanctions screening
 - The casino must ensure he does not do business with customers that are subject to international transactions
 - Before doing business or performing incidental transaction with a player the casino should check published lists of known or suspected terrorists or other sanctioned persons or companies:
 - U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons List [Specially Designated Nationals And Blocked Persons List \(SDN\) Human Readable Lists | Office of Foreign Assets Control \(treasury.gov\)](#)
 - EU Sanctions List <http://www.sanctionsmap.eu/#/main>

Identification and verification

3. Carry out verification using reliable, independent source documents, data or information to determine the player is who he claims to be

- Documents to be used (unexpired government-issued document containing photographic evidence)
 - Driver's license
 - Identification card
 - Travel document or passport

Identification and verification

- For verification of residential address the casino operator can obtain any of the following documents not older than 6 months old
 - Bank statement
 - Utility bill
 - Correspondence from a central or local government authority, department or agency
 - A rental or lease agreement
 - Contacting player by telephone, letter or e-mail
- Documents should be authentic, clear, legible and of good quality

Identification and verification

- Other verification methods are:
 - Geo-location information
 - IP address data
 - Funding method data
 - Technological measures and controls e.g. biometric checks
- If inconsistencies in information provided by player is detected, the casino should consider whether additional identification and verification measures are required

Identification and verification

4. Carry out CRA and PEP-status screening

- Carry out a Customer Risk Assessment (CRA) to have sufficient information available to detect unusual activity in the course of the business relationship
- PEP-status screening
Special requirements apply for PEPs and their family and closed associates (see enhanced due diligence)

Identification and verification of the Beneficial Owner

- This can be achieved by the terms and conditions a registering player has to explicitly accept together with a declaration in the form of a tick box that the player is registering on his own behalf
- In majority of cases the casino will not encounter situations involving beneficial owners

Obtaining information on the purpose and intended nature of the business relationship

- Within the context of the gaming sector the purpose behind opening an account or joining player's club is self-evident
- Since development of customer profile is required, the casino must, where necessary, collect documentation to establish player's source of wealth
- Where risk is not high a declaration of player can suffice (nature business/employment, annual salary)
- Social media can also be used as a source of information
- Where risk is high the information obtained need to be proved by independent and reliable information and documentation

On-Going Monitoring

- In carrying out on-going monitoring of a business relationship, the casino operator has to:
 - Ensure that documents, data and information collected under the CDD process is kept up-to-date and relevant
 - Obtain fresh documents when expiry date of identification documents held on file is reached
 - Question the data and information already in its possession whenever any inconsistencies arise
 - Scrutinize the transactions undertaken throughout the course of the business relationship to ensure they are consistent with the casino operator's knowledge of player and the player's business and risk profile, including, where necessary, the source of funds

On-Going Monitoring

- Where player's activity is not in line with what the casino operator knows or expects from the player it has to:
 - Establish the source of funds; or
 - Revise the risk profile of the player and if applicable collect the player's source of wealth
- Decide whether transaction is an unusual transaction and need to be reported to the FIU
- When monitoring all accounts held by a player with the casino operator should be linked
- The casino operator should be able to detect opening of accounts by the same customer, but using third party identities

Inability to complete CDD

- Where unable to comply with these requirements the casino operator should not open the account, commence business relations or perform the transaction
- If already a business relation the casino operator should terminate the business relationship
- Casino operator also has to make an unusual transaction report to the FIU if presumption of ML/TF/PF exist

Enhanced Customer Due Diligence

- In circumstances where risk of ML or TF is higher → enhanced CDD measures **have to** be taken to mitigate the increased risk
- These circumstances refer among other things to:
 - Politically exposed persons (international and domestic)
 - New technologies
 - Higher-risk countries
 - Other potentially higher-risk situations
- In high-risk situations the casino can consider the collection of additional information as necessary to mitigate the higher risk

Enhanced Customer Due Diligence

- These could include:
 - Obtaining additional information on the player (e.g. occupation, volume of assets info through public databases, internet etc.)
 - Updating more regularly the identification data of player
 - Obtaining information on the SoF or SoW of the player
 - Obtaining information on the reasons for intended or performed transactions

Enhanced Customer Due Diligence

- Obtaining the approval of senior management to commence or continue the business relationship
- Conducting enhanced monitoring of the business relationship , by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- Requiring the first payment to be carried out through an account in the player's name with a bank subject to similar CDD standards

Simplified Customer Due Diligence

- When risk of ML or TF are lower → simplified CDD measures, which should take the nature of the lower risk into account, **could be** allowed
- Examples of possible measures are:
 - Verifying the identity of player and the BO after the establishment of the business relationship
 - Reducing the frequency of customer identification updates
 - Reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold
 - Not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established
- Simplified CDD measures are not acceptable whenever there is suspicion of ML or TF, or where higher-risk scenarios apply

Reporting of unusual transactions

- Casinos to report unusual transactions or intended transactions to the FIU
- Unusual transaction is a transaction or series of transactions inconsistent with the player's profile
- Objective and subjective indicators established to assess whether transaction is unusual
- Unusual transactions along with supporting documents to be reported to CO
- CO to report unusual transactions to the FIU

Reporting of unusual transactions

As per annex F Ministerial decree indicators unusual transactions the following are deemed unusual transactions are:

Objective indicators

- ML/TF Transactions reported to police or judicial authorities
- An intended transaction of a natural or legal person on a UN or EU Sanctions list
- A transaction $\geq$ Naf. 5,000
 - A bank transaction $\geq$ Naf. 5,000
 - The sale of chips or credits $\geq$ Naf. 5,000
 - Payment of prizes $\geq$ Naf. 5,000

Reporting of unusual transactions

Subjective indicator

- A transaction of which there is a reason to assume that it may be possibly related to ML or TF
- Reports to be submitted via goAML portal at <https://portal.fiucuracao.cw>
- Companies to register to get access to the portal
- Reports to be submitted in English

Reporting of unusual transactions

Procedure for reporting

- Reports of objective indicators to be submitted within 48 hours of transaction taking place
- Reports of subjective indicators
 - Internal reporting to CO $\leq$ 24 hours
 - CO has 10 working days to complete relevant research
 - If presumption of ML/TF exists, CO to report within 48 hours to the FIU

Reporting of unusual transactions

- FIU annual reports 2016 -2019 and 2020-2022 indicate:
 - ‘Subjective reports are very important for the FIU, since these reports normally give a lot of information to the FIU’
 - ‘It is up to the CO of the reporting entity, who know their clients best and have more information about the situation surrounding the reported transaction, to decide if a transaction may be possibly related to ML or TF’

Reporting of unusual transactions

- Examples of situations that may be possibly related to ML or TF
 - Setting up dozens of betting accounts, with deposits well below reporting threshold to withdraw the money after a short while
 - Regularly depositing or transacting similar amounts of cash
 - Funding casino account with credit and debit cards, prepaid cards, checks and cryptocurrency and then ask for pay out
 - Unexplained income inconsistent with financial situation/customer profile
 - Customers claiming machine credits/payouts with no jackpot
 - Association with multiple accounts under multiple names
 - Frequent betting transactions just under threshold
 - Cash deposits/withdrawals just under threshold

Reporting of unusual transactions

- Parallel Even money betting
- Betting against associates / Intentional losses, where money launderers deliberately lose to one of the party who is able to receive a casino issued check or wire transfer of legitimate winnings (poker, roulette)
- Multiple currency exchanges
- Currency exchange for no reasonable purpose
- Currency exchanges with low denomination bills for high denomination bills
- Currency exchanges with little or no gambling activity
 - Wire transfers /currency exchanges just under thresholds
 - Frequent 'cash out' transactions without corresponding 'buy in' transactions or vice versa

AML Compliance Program

Elements of an AML compliance program:

- System of internal policies, procedures and controls
- Designated compliance officer
- Employee screening and training program
- Independent audit function

System of internal policies, procedures and controls

- Policy statement
- AML/CFT operating procedures translating policy in acceptable workable practice
- Internal controls

Relevant:

- Board approved
- Communicated to employees



Designated compliance officer

- AML program
- Verification of compliance with law and policies and procedures
- Training employees
- Internal / external UTRs
- Management reporting

Relevant: job description



Employee screening program and training program

- Screening employees for criminal records
- Developing training programs

Relevant:

- Different training for different employees
- Refreshment training
- Training records



Independent audit function

- Annual internal / external independent audit of AML/CFT compliance program
- Minimum required coverage in regulations

Relevant:

- Reporting to Board
- Assessment of responsiveness to audit findings



Record keeping requirements

FATF recommendation 11

All necessary records on transactions are required to be maintained for 5 years.

All records obtained through CDD must be kept for a minimum of 5 years after the business relation has ended / after an occasional transaction.

Records must enable reconstruction of individual transactions.

Examples:

- Records of player identification documents
- Communication with players and (results of) analyses of player and player transactions
- Player risk profile
- Internal / external UTRs and supporting documents thereof

Other requirements

- BRA
- CRA
- AML/CFT policies, procedures and controls
- Examination of third party (if any) to which CDD is outsourced
- Proof of FIU registration
- Internal / external UTRs and supporting documents
- Job description compliance officer
- Management reporting from compliance officer
- Employee screening program and screening records
- AML/CFT training plan and training records
- Independent audit report on AML compliance program

Requirements GCB examination

Reference: Regulation V.6





The Asia/Pacific Group on Money Laundering



Financial Action Task Force

Groupe d'action financière



FATF Report

Vulnerabilities of Casinos and Gaming Sector

March 2009



THE FINANCIAL ACTION TASK FORCE (FATF)

The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit the website:

WWW.FATF-GAFI.ORG



ASIA PACIFIC GROUP ON MONEY LAUNDERING

The Asia/Pacific Group on Money Laundering (APG) is an autonomous and collaborative international organisation founded in 1997 in Bangkok, Thailand consisting of 39 member jurisdictions and a number of international and regional observers. The member jurisdictions and observers of the APG are committed to the effective implementation and enforcement of internationally accepted standards against money laundering and the financing of terrorism, in particular the Forty Recommendations and Nine Special Recommendations on Terrorist Financing of the Financial Action Task Force (FATF).

For more information about the APG, please visit the website:

WWW.APGML.ORG

© 2009 FATF/OECD and APG. All rights reserved

No reproduction or translation of this publication may be made without prior written permission.

Applications for such permission, for all or part of this publication, should be made to the FATF Secretariat, 2 rue André Pascal 75775 Paris Cedex 16, France

(fax +33 1 44 30 61 37 or e-mail: contact@fatf-gafi.org).

TABLE OF CONTENTS

EXECUTIVE SUMMARY	7
INTRODUCTION.....	9
Scope of Research	9
Project scope / methodology	11
CHAPTER 1: THE CASINO SECTOR.....	13
Introduction	13
Regional Overviews	14
Conclusion.....	21
CASINO SECTOR RISK ASSESSMENTS FOR MONEY LAUNDERING & TERRORIST FINANCING.....	22
The need for casino sector-specific risk assessments.....	22
Guidance on Typologies Risk Assessments.....	22
Sources of information	23
Risks for jurisdictions without a casino sector.....	23
Models for casino sector risk assessments	23
CHAPTER 2: MONEY LAUNDERING METHODOLOGIES AND INDICATORS.....	25
Broad risks in casinos.....	25
Criminal interest in casinos – players and infiltration of casinos.....	26
Money laundering methods and techniques in Casinos	27
Casino value instruments	28
Indicators of ML using casino value instruments	31
Structuring.....	33
Refining.....	33
Indicators of ML using structuring/refining methods	34
Casino accounts & facilities.....	36
Indicators of ML using casino accounts:.....	38

Winnings	39
Indicators of ML using winnings:	40
Currency exchange	41
Indicators of ML using currency exchange:	41
Employee complicity	42
Indicators of employee complicity:	42
Credit cards / debit cards	43
Indicators of ML using credit/debit cards:	44
False documents	45
Indicators of ML using false documents and counterfeit currency:	45

CHAPTER 3 – SECTOR VULNERABILITIES AND EMERGING ISSUES 47

Introduction	47
Casino-based Tourism – “Junkets”	47
Vulnerabilities	48
Terrorist Financing	57

CHAPTER 4 - POLICY IMPLICATIONS 58

Online gaming / online casinos	58
Lack of AML/CFT coverage for casino sectors	58
Lack of regulatory tools	58
Implementation of CDD measures	59
Application of AML/CFT controls to casino foreign branches, offices or subsidiaries	59
Application of AML/CFT controls to casino foreign holding accounts	59
Control of junket operators and their agents	59
Regulatory controls over VIP rooms and related facilities	60
Regulatory coverage of ‘foreigners only’ casino models	60
Regulatory control over high-seas gaming	60
Controls over significant contractors, systems and equipment	60
Lack of AML/CFT capacity / experience by casino regulators	60
Coordination between AML/CFT and casino-sector supervisors	61
Building compliance culture in casino sectors	61
Law enforcement / FIU / Regulator access to information and investigation of ML/TF	62
International Cooperation	63
Conclusion	63

BIBLIOGRAPHY	65
ACRONYMS AND ABBREVIATIONS & GLOSSARY	67
GLOSSARY OF COMMON CASINO TERMS	68
APPENDIX 1. REGIONAL DATA ON CASINO SECTORS.....	69

EXECUTIVE SUMMARY

The vulnerability of casinos was recognised in the revision of the FATF 40 Recommendations, with obligations on casinos being significantly enhanced. However, there remained a lack of recent regional or global typologies on casinos and gaming, which this report seeks to address.

This APG/FATF report considers casinos with a physical presence and discusses related money laundering (ML) and terrorist financing (TF) methods, vulnerabilities, indicators to aid detection and deterrence, international information exchange. The report considers vulnerabilities from gaps in domestic implementation of anti-money laundering / combating the financing of terrorism (AML/CFT) measures. Data in the report was derived from members of the FATF, APG, other FSRBs and open sources.

Online gaming and illegal gambling are beyond the scope of this study.

Overall, there is significant global casino activity that is cash intensive, competitive in its growth and vulnerable to criminal exploitation. This paper identifies significant gaps in awareness of ML typologies, gaps in regulatory and law enforcement responses, gaps in online gaming typologies, issues with controls over junkets / VIP programs, and significant issues with controls over ‘high seas’ gaming. The report identifies significant gaps in global coverage of AML/CFT controls over the sector, which represents a significant vulnerability. The report is a resource for policy formation.

The report identifies significant ML vulnerabilities and related case studies and typologies, but does not identify any instances of TF through the sector.

Chapter 1, *The Casino Sector*, presents a global overview of casinos organised by regions (some 100 countries). The overview sets out the numbers, locations and, in some cases, ownership of each sector and coverage of AML/CFT controls. The chapter discusses some statistics and estimates of revenues (over USD70 billion globally) and profits (where known). The chapter discusses emerging casino markets, including a number of developing countries with governance and capacity challenges.

Chapter 1 briefly discusses casino sector risk assessments as a basis for allocating regulatory and law enforcement resources. The report highlights the need to identify ML risks for both those jurisdictions with or without a casino sector.

Chapter 2, *Money laundering Methodologies and Indicators*, considers vulnerabilities such as casino chips, casino cheques, casino accounts and facilities, structuring through the casino, currency exchange, employee complicity, etc. The paper describes typologies, case studies, and includes a summary of practical indicators for the industry, regulators and law enforcement.

Casinos undertake high volume/speed financial activities that are similar to financial institutions, but in an entertainment context. Casinos are generally large cash-based businesses. Foreign exchange facilities and reduced transparency of ‘high rollers’ in VIP rooms present substantial challenges. The use of foreign holding accounts where funds in one jurisdiction are available for use in a casino in another jurisdiction without the need for a cross border remittance presents further issues.

Chapter 3, *Sector Vulnerabilities and emerging Issues*, explores a number of additional

vulnerabilities and emerging issues. Casino-based tourism or “junkets” are identified as a vulnerability as they involve the cross border movement of people and funds and often target high net-worth / VIP clients. Transparency of the movement of funds is an issue with junkets, due to gaps in controls, and weak implementation and supervision.

The emerging issue of high-seas cruise ship casinos and associated junkets is a challenge for regulators and law enforcement. The question of who has jurisdiction is prominent, including where the vessel is registered, where it operates from and where it visits. The paper notes that few jurisdictions regulate this sector.

With respect to VIP rooms and ‘high roller’ customers, vulnerabilities are noted with identifying source of funds and movement of funds. In many casino markets high-roller clients make up a large majority of casino turnover, yet only a very small percentage of casino patrons.

Other vulnerabilities discussed include corrupt or inadequately trained staff, new markets opening and terrorist financing.

Chapter 4, *Policy Implications*, reiterates various key findings of the report and discusses a number of policy implications, including:

- Online gaming requires further typologies study and sharing of cases and regulatory models is needed;
- A significant number of jurisdictions do not subject their casino sector to AML/CFT controls;
- When casinos are subject to AML/CFT controls, many jurisdictions lack effective implementation of preventative measures (CDD, STRs, internal controls);
- There is a lack of regulatory tools that carry effective, proportionate and dissuasive sanctions;
- AML/CFT controls over casino foreign branches, offices or subsidiaries are not well regulated and there is a need for international guidance and best practice;
- Casino foreign holding accounts are not clearly covered for AML/CFT, which allows movement of funds without sending a cross-border wire transfer;
- Controls over VIP rooms vary and some jurisdictions lack clear powers regarding collecting and sharing information of VIP program participants;
- High-seas gaming is a large market over which there is little regulatory control;
- Many jurisdictions’ casino regulators lack AML/CFT capacity and experience;
- International cooperation between casino regulators on AML issues is lacking and it is not always clear who are the competent authorities for information sharing.

INTRODUCTION

1. The APG and FATF have undertaken a joint study of vulnerabilities in the gaming and casinos sector. The project is led by New Zealand, with Ms Rachael Horton of New Zealand Department of Internal Affairs leading the work, including the drafting of this report. The work arose due to FATF and APG mutual evaluations and earlier typologies work, which noted a range of ML/FT risk factors related to gaming and casinos.

2. The project has examined and illustrated areas of vulnerabilities in the gaming and casino sectors with an emphasis on legal sectors that have a physical presence. The project has sought to identify sector-specific money laundering or terrorist financing indicators; and to highlight possible policy implications for effective implementation of the FATF standards to cover casinos and gaming.

Scope of Research

3. Typologies produced by the FATF and APG over the last 10 years have consistently identified a money laundering risk from casinos and gaming. The casino and gaming sector is characterised by diverse types of gambling activity, size and rate of development, as well as public and private sector ownership models.

4. Within the sector, the FATF recognised that casinos represent the greatest risk for money laundering activities and this was reflected in the revision of the FATF 40 Recommendations 2003, with obligations on casinos being significantly enhanced in relation to Customer Due Diligence (CDD), record keeping, reporting of suspicion, and comprehensive regulation and supervision.

5. Casinos are the only form of gaming or gambling explicitly covered by the FATF standards, however the FATF standards do not define casinos or gaming, nor do they set out the activities undertaken by casinos. It is left to each jurisdiction to determine the forms of gaming included in its coverage of “casinos”.

Magnitude of casino sector globally

6. Statistics from 2007 show that over 150 countries participate in some kind of legal gambling, 100 of those countries have legalised casino and card room gambling. Over 100 countries offer some kind of lottery product and over 60 countries participate in the race and sports betting industry.¹

7. Casinos generate enormous revenue streams for providers and for government through taxation and licensing fees. The size of the global casino business was estimated at over USD 70 billion in revenue in 2006, although a figure for overall turnover of funds was not available. Casinos in North America (US and Canada) account for almost half of that figure. Macao China is the fastest growing casino jurisdiction, and recorded more than USD 10 billion in gaming revenue in 2007. In addition there is a proliferation of Internet gambling sites, with global revenues estimated

¹ “Overview of Gaming Worldwide”, *Casino City, Global Gaming Almanac*, 2007, <http://www.casinocitypress.com/GamingAlmanac/globalgamingalmanac>.

around USD 15 billion,² plus a significant amount of illegal gambling occurring around the world, which is largely unmeasured.

8. The nature and expanding scope of the casino sector presents a number of challenges for AML/CFT implementation. In particular:

- Casinos are cash intensive businesses, often operating 24hrs per day, with high volumes of large cash transactions taking place very quickly.
- Casinos offer many financial services (accounts, remittance, foreign exchange, cash issuing etc), but in some jurisdictions may only be regulated as ‘entertainment’ venues, rather than financial institutions.
- In some jurisdictions casinos are poorly regulated or unregulated for AML/CFT.
- A number of jurisdictions with well regulated casino sectors continue to identify significant levels of money laundering.
- Many casinos are located in geographic areas characterised by poor governance, political instability or bordering regions with significant crime or terrorist problems.
- The movement of funds associated with gaming-related tourism is poorly understood and may pose particular money laundering risks, e.g. international movement of funds for casino ‘junket’ operations³.
- In some jurisdictions casino staff turnover is high, sometimes due to seasonal factors, which can lead to weaknesses in staff training and AML/CFT competencies.

9. A significant number of countries have recently established, expanded, or are considering expanding their gaming and casino sectors.

10. In response to these issues the FATF and APG began a project to consider money laundering and terrorist financing vulnerabilities in the Casino and Gaming sector.

11. This paper examines ML and TF vulnerabilities with legally operating casinos. The paper does not consider issues related to online gaming, but rather is concerned with casinos that have a physical presence. The aim of the project is to share information on the casino sector for the following purposes:

- Assist jurisdictions to understand money laundering and terrorist financing methods.
- Increase understanding in the casino sector of money laundering and terrorist financing vulnerabilities.

² “eGaming Data Report: Global Internet Gambling Revenue Estimates and Projections”, *Christensen Capital Advisors 2005*, <http://www.cca-i.com>.

³ The term Junket has its origins in Chinese where Jin literally means introducing and Ke means customers. It is a method of casino marketing developed in the late 1930s for introducing customers to the expanding Macao, China gaming industry. Over time this method has been adopted elsewhere and the term has gradually evolved to be known as Junkets.

- Assist law enforcement and gatekeepers in the industry to detect and deter forms of money laundering.
- Strengthen capacity and international information exchange.
- Provide evidential basis to support domestic implementation of AML/CFT measures in the sector.

12. The following chapters will:

- Examine the scope and nature of regional casino sectors.
- Identify and examine money laundering methodologies from known cases.
- Identify related indicators to support operational and policy objectives.
- Examine sector vulnerabilities and emerging issues.
- Highlight possible policy implications for effective implementation of the revised FATF 40 + 9 recommendations to cover casino operations.

13. Unless otherwise referenced, all data contained in this report is sourced from jurisdictional reports and research questionnaires submitted to APG and FATF.

Project scope / methodology

14. The APG began initial work on money laundering typologies in the casino sector in November 2006 during the Annual Typologies Workshop in Jakarta. At that time the APG commenced some preliminary scoping work and a number of APG jurisdictions shared their experience of AML/CFT issues in casino and gaming sectors.

15. The 2007 FATF/APG Typologies Meeting included a workshop on casinos and gaming. The workshop was very well supported by members of the FATF, APG and other FSRBs. The following jurisdictions were involved in the 2 day breakout session which considered issues in depth: Australia; Austria; Belgium; Canada; Ireland; Japan; Netherlands; New Zealand; Spain; United States; China; Hong Kong, China; India; South Africa; OECD; Cambodia; Macao, China; Malaysia; Papua New Guinea; Philippines; Thailand; and Vietnam.

16. Following on from the workshop in Bangkok, the FATF and APG distributed a short survey to FATF and FSRB members. The survey results were in addition to materials provided by APG member jurisdictions. The following jurisdictions provided a response to the survey:

Austria	Latvia	Spain
Belgium	Malta	Sweden
Brazil	Mexico	Ukraine
Finland	Poland	United Kingdom
Germany	Romania	
Iceland	Slovenia	

17. This project would like to acknowledge the particular input of New Zealand (Department of Internal Affairs), Australia (NSW Casino Control Authority and AUSTRAC); Canada (RCMP); Macao, China (Gaming Inspection & Coordination Bureau and Financial Intelligence Office); Hong Kong, China; Belgium; Austria; Spain; Vietnam; US; and the OECD.

CHAPTER 1: THE CASINO SECTOR

Introduction

18. There is very wide range of legal gaming / gambling across the globe. This includes various games of chance and gambling forms ranging from casino and card room gaming, lotteries, online gaming, race and sports wagering and charitable gaming, such as raffles, bingo and other low technology games. Legalised gambling has become more prevalent over the last 25 years as more jurisdictions take advantage of the revenue sources from the taxation and regulated gambling industries. Over this time many governments have allowed for the expansion of legal gambling, including casinos, or introduced regulatory regimes over existing gambling.

19. Based on information generated by the gaming sector, it is estimated that over 150 countries participate in some form of legal gambling and 100 of those countries participate in legalised casino and card room gambling. The broad AML/CFT network of FATF and FATF-style regional bodies includes over 180 jurisdictions globally. At least 77 of these 180+ jurisdictions have been identified from the responses to research questionnaires and other requests for information, as having legally operating casino sectors.

20. *Appendix I* provides summary tables of each the casino sectors operating in each region.

21. The casino market is in a major growth phase in most regions. At least three jurisdictions (Albania, Singapore and Papua New Guinea) have newly passed legislation and a greater number have recently expanded their casino sectors (South Korea; Macao, China; and Chile are examples). At least five jurisdictions have been identified as taking active steps towards legalising or giving consideration to legalising casinos (see section Emerging Markets).

22. A number of jurisdictions report significant problems from illegal gaming. Illegal gaming is largely beyond the focus of this study. It is recognised that illegal gaming is a factor in governments considering regulated gambling. A number of jurisdictions have casinos operating outside of legal frameworks. These include Sri Lanka (not clearly legal) and Myanmar.

23. A number of countries, recognising the social harms associated with gambling, have recently moved to restrict gambling growth in an effort to curb rising social costs (UK in relation to its 'super' casino and Russia through its four designated gaming zones).

24. There are a significant number of jurisdictions where gambling is illegal for religious and other reasons. In a number of these jurisdictions proponents are making a case for legal and regulated gambling to be introduced.

Regional Overviews

Africa

25. Sector studies view Africa as a significant growth region for casinos. This is the case in both the major casino market in South Africa and in smaller developing markets in other African jurisdictions. A number of casino jurisdictions in Africa do not regulate the sector for AML/CFT and a greater number appear to be poorly regulated. A number of jurisdictions have sought to restrict casinos only to foreigners.

26. Based on information from FSRBs, commercial databases and commercial studies casinos are known to be legally operating in Egypt (25), Morocco (8+) and Tunisia (4) (MENAFATF members).

27. Casinos operate in Cameroon (3), Central African Republic (2), Gambia, Ghana (3), Liberia (1), Mali (1) and Senegal (4) (all GIABA countries). Casinos operate in Botswana (11), Comoros (3), Kenya (15+), Malawi (1+), Mauritius (7+), Mozambique (3), Namibia (3), Seychelles (3), Swaziland (5+), Tanzania (7+), Uganda (3), and Zimbabwe (6) (ESAAMLG region).

28. South Africa is the only FATF member of this region and has over 40 legal casinos operating, making it by far the biggest casino sector in Africa. Casinos in South Africa are covered by AML/CFT controls. There are a number of cases reported in the press of criminals attempting to launder proceeds of crime through one or a number of South Africa's casinos.

Middle East

29. Online commercial directories⁴ list casinos operating in Iraq and Lebanon (1), both jurisdictions members of MENAFATF, but the nature and extent of casino gambling in these countries is unknown. Israel operates licensed cruise-ship casinos as well as land-based casinos.

Asia/Pacific

30. The Asia/Pacific region has the world's fastest growing economies, the world's strongest growth in tourism, and a vast array of cultures, languages, religions, political structures and consumer preferences. The region is also characterised by significant differences in wealth distribution ranging from well developed economies with strong governance and AML/CFT controls to some geographic areas characterised by poor governance, political instability or bordering regions with significant crime or terrorist problems. Some legal casino sectors are located in jurisdictions that have predominant cash-based economies and weak regulatory controls and/or no controls for AML/CFT. These factors present a significant challenge for governments and regional bodies committed to ensuring effective AML/CFT controls.

31. Within Asia there are legal casino sectors in: Korea (17); Lao PDR; Macao, China, China (29); Malaysia (1); Nepal (6); Philippines (14); and Vietnam (2). Sri Lanka has nine large casinos which are not regulated and are not subject to AML/CFT controls, but pay a levy to the government to operate pursuant to the Betting and Gaming Levy Act. Casinos in India are only permitted in one state and are not yet subject to AML controls. Press reports from late 2005 noted a draft bill had been prepared to regulate casinos in Nepal but this has not been enacted. Casinos in the Philippines are

⁴ Casino City.

regulated, but there is no competent authority for AML/CFT matters, although the Philippine Amusement and Gaming Corporation (PAGCOR) have voluntarily agreed to submit suspicious transaction reports (STRs) to the Anti Money Laundering Council.

32. There is a mix of state and private ownership of casinos across the region. For example, in the Philippines, all casinos are state owned.

33. Some jurisdictions, such as Cambodia (21), Korea, Nepal and Vietnam restrict citizen access to casinos, only permitting foreign tourists to enter the casinos and gamble.

34. Hong Kong, China does not have a legal casino sector; many residents favouring travel to Macao, China due to its proximity and ease of access. Although the operation of casinos is illegal within the jurisdiction, Hong Kong, China is the home port for several cruise ships offering cruises into international waters principally to provide casino operations (see Chapter 3 for more information on ‘high seas gambling’).

35. Singapore is due to open its first casinos in 2009. Jurisdictions considering legalising casino gambling include Indonesia, Japan, Palau, Chinese Taipei, Thailand and Timor Leste (see box 2 below).

36. Casinos are illegal in Bangladesh, Brunei Darussalam, China, Chinese Taipei, Indonesia, Mongolia, Myanmar, and Pakistan.

Box 1. A Closer Look at Macao, China

Macao, China is a Special Administrative Region of China. Macao, China's population is just 0.5 million. The majority of the economy is linked to the tourism and casino industries. The casino industry now outstrips Las Vegas with casino revenue. Tax collected in 2008 made up over 70% of government total revenue. Macao, China holds the monopoly over casino-style gaming in the region with 31 casinos in operation.⁵ There are approximately 30 million total visitor arrivals in 2008. Over half are from mainland China, the remaining predominantly from Hong Kong, Chinese Taipei and South East Asia. In 2002 Macao, China ended the gaming monopoly which had been dominated by Mr Stanley Ho's *Sociedade de Turismo e Diversões de Macao, China* (STDM) for 40 years. It liberalised the gaming industry by granting three casino gaming concessionaires and 3 sub-concessionaires.

The competent authorities responsible for the regulation of the casino sector are the Gaming Inspection and Coordination Bureau (DICJ) and the Judiciary Police. Criminal investigation of money laundering activities is undertaken by the Judiciary Police, whilst the preventative measures against money laundering are the responsibility of the DICJ. For currency exchange activities inside the casinos, they are under the supervision of the Monetary Authority of Macao.

Macao, China has introduced a licensing system to regulate junket operators. All licensed junket operators are obliged to file their information with the government, with their names published in the Official Gazette. Their licence will be reviewed periodically to see whether they are properly complying with the legislation and see whether they still fit the requirements of a junket operator. All casinos, junket operators and currency exchange counters inside the casinos have the duty to report Suspicious Transaction Reports to the Financial Intelligence Office of Macao, China. At the same time, casinos and junket operators have to submit large transaction reports to the Gaming Inspection and Coordination Bureau.

37. There are seven jurisdictions with legal casino sectors in the Pacific. These include Australia (13), New Caledonia, New Zealand (6), Northern Mariana Islands, La Réunion (France), Solomon Islands, and Vanuatu (1). Papua New Guinea passed legislation in 2007 for 23 land-based and online

⁵ As at September 2008, reported by The Gaming Inspection and Coordination Bureau.

casinos and Palau and Timor Leste are considering legalising casinos. All of the jurisdictions with casino sectors or considering legalising casinos are APG members, except for New Caledonia, Northern Mariana Islands, and, La Réunion (France). Casinos are not operating in Niue, the Cook Islands, Fiji, Tonga or Samoa.

38. Cruise ships operating in the Pacific include offshore gaming, but do not operate while in harbour on pacific islands. Pacific jurisdictions indicate that they lack clear information on the operation and regulation of these gaming cruise ships.

39. Australia is the largest casino sector in this region with 13 legally operated casinos, the first opening in Tasmania in 1973, and each state and territory having a least one. The casinos vary in size from 18 tables and 250 gaming machines to 350 tables and 2 500 gaming machines. Total gaming revenues from Australian casinos was recorded as AUD 2.8 billion in 2005/06.⁶ Gaming revenue, the largest component of casino revenue, has experienced a 4.1% cumulative annual growth and average annual growth rate since 2002/03. Each state and territory has its own regulatory and licensing control over casinos, which includes investigation and enforcement. In addition, all casinos are classified as “regulated entities” under law and supervised by the FIU (AUSTRAC) for compliance to AML/CFT laws. Casinos are commercially owned and operated in Australia and open to both citizens and tourists.

40. New Zealand has six legally operated casinos, the first opening in 1994. Gambling revenue in casinos was reported at NZ469 million in 2007.⁷ They are all commercially owned and operated and open to both citizens and tourists. New Zealand, however, does not have AML/CFT supervision of casinos, but has draft legislation underway to rectify this. Current laws provide financial reporting responsibilities to the FIU. General casino supervision is the responsibility of the Department of Internal Affairs, but casino licensing is the responsibility of a separate Gambling Commission. In 1997 the New Zealand Government passed a moratorium on new casinos, capping the number of legal casinos allowed to operate at six.

Central Asia

41. The Eurasian Group (EAG) report casinos operating in Kazakhstan and Kyrgyzstan (18). In Kazakhstan laws passed in April 2007 limit casinos to two provincial cities – Kapchagai and Shchuchinsk, but it is unknown if any regulation of AML controls are in place. The 18 casinos reported in Kyrgyzstan are regulated, including for AML/CFT, however a recent ME noted the casinos are showing some resistance to these laws.

42. Tajikistan, Turkmenistan, and Uzbekistan report no casinos operating, although it is uncertain if this is because of legal restrictions or market limitations.

Europe

43. Europe has long-established casino and gaming sectors and has experienced large-scale growth in recent years. Within Europe European Union (EU) members have responsibility to implement AML/CFT measures on casinos following the relevant EU directives. There are

⁶ “Australian Casino Economic Report 2005/06”, July 2007, *Australian Casino Association*, <http://www.auscasinos.com/documents/publicationsSubmissions/ACAFinalReport200506v3.pdf>

⁷ Department of Internal Affairs. *Gambling Expenditure Statistics 1983 – 2007*, [http://www.dia.govt.nz/Pubforms.nsf/URL/Expendstats07.pdf/\\$file/Expendstats07.pdf](http://www.dia.govt.nz/Pubforms.nsf/URL/Expendstats07.pdf/$file/Expendstats07.pdf)

39 jurisdictions in the Europe with reported legal casino sectors in operation. These include: Austria (12), Belgium (9), Cyprus (20+), Czech Republic (158), Denmark (6), France (161), Finland (1+), Georgia (2), Germany (62), Greece (9), Hungary (6), Italy (4), Latvia (14), Luxembourg (1), Malta (4), Poland (27), Portugal, Romania, Russia (348), Slovakia (4), Slovenia (14), Spain (39), Sweden (4), Switzerland (19), and the United Kingdom (165 licensed 140 operating). See Annex A for full details.

44. Casino ownership across Europe varies between state and private ownership, but some jurisdictions, such as Germany, Slovenia and Sweden have a mix of both. There is no citizenship prohibition reported. Most casino sectors are regulated and all are subject to AML/CFT controls. Casino jurisdictions rely less on junket or casino tourism operations and few European jurisdictions report commercial arrangements between casinos and junket promoters to support casino tourism.

45. In most European countries there exists alongside traditional casinos a low stakes gaming machine market. These machines can be found in many places, including sports betting shops and poker clubs.⁸ With regards to the size of each sector, Russia has the largest sector with 348 operating casinos. After 1 July 2009, all gaming in Russia will be prohibited except within four newly created special gaming zones in Kalingrad, Rostov-na-Donu, Altai and Primorie Krai (Vladivostok), France, the Czech Republic, and the United Kingdom follow closely with 160, 158 and 140 respectively.

46. Austria has 12 casinos which generated approximately Euro 190 million in revenue in 2007 from 2.44 million visitors. Finland has just one casino which recorded annual turnover of EUR 30.9 million in 2007. Germany has 62 casinos which generated 944 million revenue in 2005 from 7.7 million visitors. Germany's casino sector employees approximately 5 000 staff. Slot machines account for 75% of gross earnings in German casinos. Malta has three casinos which employ over 600 people. Spain has 39 casinos which attracted 3.3 million visitors in 2006.

47. Ireland has a number of private gaming clubs operating casino-like facilities that create an AML/CFT risk, but which fall outside the scope of their AML laws. Casinos are reported to be illegal in Iceland, Norway and Turkey.

South America

48. Many Central and South American jurisdictions have well established gaming sectors (lotteries, sports betting, etc) but fewer have well established casino sectors. GAFISUD and online directories report casino sectors operating in Argentina (70+), Chile (17+), Uruguay (18), Peru (7), and Venezuela (5), however it is unknown the extent of regulation and/or AML controls over these sectors. Uruguay and Venezuela also report casino sectors, but no further information is available. It is unclear the extent to which South American casinos rely on introduced junket operations.

49. Argentina has a well established gaming market with further expansion taking place in the casino sector. Casinos do not operate in Bolivia, and it is unknown if Colombia, Ecuador and Paraguay have casino sectors.

50. Bolivia and Brazil prohibit casinos.

⁸ Rich Geller. "Saturation or Malaise?" *Global Gaming Business*, June 2008, p. 40.

The Caribbean and Central America

51. The Caribbean has more than 120 casinos on 15 islands. The CFATF reports casinos operating in the Bahamas (4), Belize (2), Costa Rica (35), Dominican Republic (44), Jamaica (10), Panama (14), and Suriname (9), but the level of regulation and AML controls is not clear.

52. Trinidad and Tobago have no legal casinos but have 72 registered Private Members Clubs that operate like casinos, but are not supervised by the government.

53. Open source material reports that Panama has 14 full-scale casinos with three additional licences being recently granted, and 29 gaming machines halls. Combined with non-casino gaming revenues, Panama has the second-largest gaming market in Latin America behind Argentina. AML/CFT controls appear to be lacking in Costa Rica, El Salvador, and Nicaragua despite recent attempts by their respective governments to better control and regulate the industries. The Dominican Republic does not extend AML controls to the sector.

54. In Bermuda, the Cayman Islands, Guatemala and Guyana casinos are illegal.

North America

55. Canada and the United States account for almost 50% of the global casino market.

56. Casinos in Canada are relatively recent with most opening in the early 1990s (except for Yukon where a charity casino was legalised in 1973). Canada now has 63 casinos operating in seven provinces and one territory (Yukon). 29 of these are commercial casinos which are usually state-owned or operated through service contracts with private corporations. There are 24 charity casinos licensed in Alberta, and one in Yukon, which are all privately owned. In Alberta, only religious or charitable groups may hold a casino licence. Also in Canada there are nine First Nations⁹ casinos operating in Ontario, Manitoba and Saskatchewan. The provincial and territorial authorities are responsible for regulating all casinos, as well as municipal, provincial and federal law enforcement agencies. The Canadian FIU (FINTRAC) is responsible for ensuring that casinos are compliant with their responsibilities under AML/CFT laws.

57. Cruise ships operate out of Canadian waters and do offer casino facilities (except within five nautical miles of a Canadian port). As with many FATF/APG jurisdictions AML/CFT measures do not apply to cruise ship gambling.

58. The 2005 revenues and profits for commercial and charity casinos in Canada are shown in Table 2 below:

Table 1

	Revenues 2005	Profits 2005
Commercial Casinos	CAD 3.7 billion	CAD 1 billion
Charity Casinos in Alberta	CAD 1.2 billion	CAD 147 million

9. TBD.

59. The United States has approximately 845 casinos and card clubs operating in at least 30 jurisdictions (including Puerto Rico, the U.S. Virgin Islands and Tinian). Casino ownership in the United States is a mix of commercial and tribal ownership. In 2003, more than USD 800 billion was wagered at casinos and card clubs in the United States. In particular, there has been a rapid growth in riverboat and tribal casino gaming as well as card room gaming over the last ten years (see Box 5 for more on Indian Gaming in the United States). Collectively, tribal casinos took in USD 25.7 billion in revenue in 2006, compared with Nevada's revenues of USD 12.06 billion for the same year.

60. Gambling is primarily a matter of state/territory law and responsibility for regulating casinos falls on state gaming commissions and the National Indian Gaming Commission. All legally licensed casino and card clubs with gross annual revenues greater than USD 1 million are subject to Federal AML requirements in the BSA. Covered gaming establishments (state licensed land based, riverboat, tribal casinos and card clubs) are subject to AML requirements. The US FIU (FINCEN) administers the BSA but does not directly examine casino for compliance with the law. That is delegated to the Internal Revenue Service (IRS). For floating casinos, i.e. gambling "cruises to nowhere" which operate out of certain states along the East Coast of the US to conduct gambling beyond the 3 nautical miles limit, customers are subject to reporting currency and monetary instruments of \$10,000 or more when sailing both in and out of US territorial waters ships. Moreover, the operators of the "cruises to nowhere" are required to file tax notices for jackpot wins of USD 1200 or more.

Box 2. Indian Gaming in the United States

Tribal government-sponsored gaming is an evolution dating back to the late 1970's. After the Supreme Court confirmed (in 1987) the right of the tribal governments to establish gaming operations, Congress passed in 1988 the Indian Gaming Regulatory Act (IGRA) (25 USC 2701) which recognized, but limited, the right of tribes "to conduct gaming operations" and embodies a compromise between state and tribal interest. According to the IGRA, the states are given a voice in determining the scope and extent of tribal gaming by requiring tribal-state compacts for all forms of casinos style gambling and other gaming activities. Most recently tribal casinos have moved rapidly from relative obscurity within the casinos industry to prominent position with ample potential for money laundering and other types of financial crimes. There are 567 federally recognised Indian Tribes, half of which are in Alaska, and 225 of them operate 411 gaming facilities in 28 states.¹⁰ Of these 307 are considered casino operations, while the remainder are basically bingo halls. Collectively, the tribal casinos took in USD 25.7 billion in revenue in 2006, more than twice the amount generated by Nevada casinos.¹¹ If the tribal gaming industry were a single company, rather than 307 casinos, it would rank near the top 100 corporations in America. Tribal gaming interests have what is currently the largest casino in the United States, Foxwoods Resort and Casino, located in Mashantucket, Connecticut and owned by the Mashantucket Pequot Tribe. The west coast, primarily California, represents the fastest growing region for the Indian gaming industry.

61. Mexico reports a growing gaming industry; however, the only casino-style of gambling authorised is in betting game halls exclusive to regional fairs with cards, dice and roulette. These are Temporary permits for large-scale "salones de Apuestas", regulated by the Secretaría de Gobernación (Ministry of Interior), but not subject to AML controls. The Mexican government do not foresee any permanent casinos being located or permitted to operate within national territory.

¹⁰ "An Analysis of the Economic Impact of Indian Gaming in 2006", *National Indian Gaming Association*, http://www.indiangaming.org/info/pr/press-releases-2007/NIGA_econ_impact_2006.pdf

¹¹ "Tribal casino revenue up 5 percent nationwide", *Associated Press*. June 19 2008, http://blog.mlive.com/kzgazette/2008/06/tribal_casino_revenue_up_5_per.html

Emerging Markets

62. Given the scope of potential revenue and the interest in foreign direct investment, a number of regions have significant emerging markets in the casino and gaming sectors. This is particularly the case in the Asia/Pacific region and in Africa.

63. A number of developing countries with predominantly cash-based economies and weak or limited AML/CFT capacity are giving active consideration to establishing casino sectors. Some of the smaller less developed countries considering legalising casinos include Palau and Timor Leste.

64. Singapore has passed legislation which provides for granting two licences for large-scale casinos. The licensing remains subject to confirmation of suitability of the two casino operators.

65. Papua New Guinea passed legislation in 2007 for approximately 20 land-based and online casinos.

66. Japan has indicated has organised crime groups running casino-like operations for online gaming, but is giving consideration to establishing luxury casino resorts by 2012 if liberalisation of the gaming market goes ahead.

67. Chinese Taipei is considering proposals to open up the island nation's gambling business by revising legislation that may allow casinos on the offshore islands of Chinese Taipei.¹²

68. Thailand is also considering legalising gambling after the findings of a detailed study on the prevalence of illegal casinos at the border between Thailand and Myanmar and related flows of funds to neighbouring casino jurisdictions. Thailand estimates USD 4-17 billion in illegal gambling turnover annually and 100 000 people arrested per annum for illegal gaming.

Box 3. Drivers for Change in Asia

Market analysts consider that the Asia region has an undersupply of quality legal casino venues. Such analysts view Asia as having the greatest potential for growth in casino revenue and venue development. The key drivers for regulatory change in the Asia region include:

1. Economic growth resulting in increased disposable income.
2. Changing social attitudes.
3. Increased media and government attention on existing illegal gambling industries.
4. Need for increased taxation revenues.
5. Need for tourism infrastructure development.
6. Availability of private sector capital for foreign direct investment.

However, issues that drive resistance to regulatory change include:

1. Social conservatism.
2. Religion.
3. Corruption in government.
4. Incumbent illegal and legal operators.
5. Government inefficiency or insufficient capability to affect change.
6. Voter/communities lack of faith in government to effectively regulate and control the industry.

¹² Global Gaming Business, "Asia Update", June 2008, p. 30.

Conclusion

69. What is shown in this chapter and in detailed tables at Annex A is the extent of casino gambling around the world and the diversity of each region's sector. Demand for casino gambling services is high and increasing and is associated with high revenues for government. This is leading some jurisdictions to legalise gambling particularly in developing countries.

70. There are established casino sectors in jurisdictions with government oversight, but are unregulated for AML/CFT.

71. The next two chapters set out a number of vulnerabilities of casinos to money laundering by describing the methods and indicators of money laundering from past cases and the casino sector vulnerabilities and emerging AML-related issues.

CASINO SECTOR RISK ASSESSMENTS FOR MONEY LAUNDERING & TERRORIST FINANCING

The need for casino sector-specific risk assessments

72. The casinos project group considered the need to conduct periodic assessments of ML/TF risks in the casino and gaming sector. The project group discussed the benefits of understanding the nature of the ML/TF environment to allow regulatory and enforcement agencies to better allocate resources to address priority risks in the casino sector.

73. ML/TF is one aspect of criminal risk. Risk assessments of the casino sector may look at broader risks including organised crime, loan sharking, prostitution, drug dealing, human trafficking etc.

Guidance on Typologies Risk Assessments

74. The FATF WGTYP June 2008 paper on Risk Assessments identifies factors that may influence the ML/TF risk in a country and suggests information to access when conducting a risk assessment. The WGTYP paper highlights a wide range of factor to be covered in a risk assessment. For the casino and gaming sector, these may include:

- Legal and regulatory environment.
- Characteristics of the economy as well as the casino/gaming sector.
- Ownership structure, integrity, internal controls and corporate governance of casino/gaming institutions.
- Ownership structure, integrity internal controls and corporate governance of intermediaries and associated businesses (junket promoters, agents, gaming equipment, financial service providers).
- Types of products and services offered and clients served.
- Criminal activities and proceeds of crime generated domestically as well as generated abroad but laundered domestically.
- Financial services offered by casino/gaming institutions and by casino intermediaries (junket promoters, agents etc).

Sources of information

75. Responses received from FATF/APG questionnaires indicate that many jurisdictions are receiving suspicious activity reports from casinos or that relate to casino activity. Casino regulators, law enforcement, bank regulators and FIUs hold useful information to assess risk areas.

76. The project group noted that a number of commercial companies provide baseline information on national and regional casino and gaming trends, including size, scope and nature of markets; trends in investment and regulation and criminal exploitation, including money laundering. This information can assist competent authorities understand the nature of their sector as well as offshore sectors.

Risks for jurisdictions without a casino sector

77. The casinos project group discussed why and how a jurisdiction without a casino sector may undertake an ML/TF risk assessment. These may be undertaken in response to illegal gaming as well as the movement of persons and funds to another gaming jurisdiction to launder the proceeds of crime.

Models for casino sector risk assessments

78. A number of countries have recently undertaken casino sector risks assessments. The models of assessment have varied, depending on the agency undertaking the assessment and the purpose (*e.g.* policy settings, law enforcement responses, regulatory compliance).

Police-led assessment - e.g. Canada

79. Canada's RCMP has recently undertaken a police-led assessment of ML risks in the casino sector. This involved working with a very wide range of stakeholders to identify national sector-specific risks. As with other risk assessments, the RCMP drew on a wide range of information sources to understand risks in the sector. These included typologies trends derived from the FIU; interviews with operators in the sector, including staff of casinos (pit bosses, owners, security etc); and information collected from intelligence databases on related crime trends.

80. The assessment aimed to understand:

- The scope of the casino sector: number, type, location, ownership, risk profile etc of casinos.
- How Casinos are used as financial intermediaries.
- Law enforcement cases / intelligence of how casinos are used for ML or are associated with predicate offences (fraud, loan sharking etc).
- Criminal trends linked to casinos.

Academic Sectors – e.g. Thailand

81. Thailand is a jurisdiction where casinos and gaming are illegal. Thai authorities have long recognised a very significant illegal gaming problem and the large scale movement of Thai nationals to foreign casino jurisdictions.

82. In order to better understand background issues, Thailand sought the assistance of the academic sector to undertake a scoping study of the impact of illegal gaming on Thailand, including ML and TF risks to the country. Thai authorities have given some consideration to regulatory reform and the possible licensing of some forms of gaming, including casinos.

83. The scope of the Thai assessment included the value of gaming sector (illegal and offshore gaming); scope of illegal gaming; movement of Thai people to foreign jurisdictions for gaming; risks for ML/TF and other predicate offences (smuggling, drugs, human trafficking etc); and impact on the community from illegal gaming.

- Over 100 000 people are arrested each year for illegal gambling offences.
- It is estimated that there are 200 to 300 illegal gambling houses in Bangkok.
- Annual turnover for illegal gambling houses in Bangkok is estimated at between USD 4 to 17 billion and for those outside Bangkok is USD 2 to 4 billion.
- There are 27 legal or semi-legal casinos operating in neighbouring countries within very close proximity of the Thai border servicing Thai gamblers.
- Thai junket operators offer casino tourism services in major Thai cities to move people and funds to these ‘offshore’ casinos.
- Movement of Thai citizens to border casinos increases risks associated with currency smuggling and cross-border crime risks including smuggling, human trafficking and drug trafficking.

Regulator-led assessments – e.g. Australia

84. In Australia, AUSTRAC, as the AML/CFT regulator, and various state-based casino regulators have worked together to conduct a preliminary assessment of key typologies and regulatory risk related to money laundering and terrorist financing. This has involved considering a range of law enforcement information, regulatory information and sector information to identify areas of specific risk and to supporting preparation of AML guidelines and AML/CFT supervision and monitoring.

CHAPTER 2: MONEY LAUNDERING METHODOLOGIES AND INDICATORS

85. This chapter will identify and examine money laundering methods from known cases and draw out related indicators to support the detection of money laundering activity.

Broad risks in casinos

86. Casinos are by definition non-financial institutions. As part of their operation casinos offer gambling for entertainment, but also undertake various financial activities that are similar to financial institutions, which put them at risk of money laundering. Most, if not all, casinos conduct financial activities akin to financial institutions including: accepting funds on account; conducting money exchange; conducting money transfers; foreign currency exchange; stored value services; debit card cashing facilities, cheque cashing; safety deposit boxes; etc. In many cases these financial services are available 24 hours a day.

87. It is the variety, frequency and volume of transactions that makes the casino sector particularly vulnerable to money laundering. Casinos are by nature a cash intensive business and the majority of transactions are cash based. During a single visit to a casino a customer may undertake one or many cash or electronic transactions, at either the ‘buy in’ stage, during play, or at the ‘cash out’ stage.¹³ It is this routine exchange of cash for casino chips or plaques¹⁴, TITO tickets¹⁵, and certified cheques, as well as the provision of electronic transactions to and from casino deposit accounts, casinos in other jurisdictions and the movement of funds in and out of the financial sector, which makes casinos an attractive target for those attempting to launder money.

88. As this research is solely focused on casinos, the data collected is not wide enough to carry out statistical trend analysis. Chapter 3, however, does provide specific sector vulnerabilities and emerging issues as a start to this broader study. It is also recognised that methods and indicators are immediately useful to private sector organisations seeking to develop effective AML/CFT processes.

¹³ The ‘buy in’ stage is when a customer enters a casino and purchases casino chips, tickets, or gaming machine credits in order to commence gambling. The ‘cash out’ stage is when a customer converts casino chips, tickets or gaming machine credits for cash, casino cheque, credits an account or transfers funds to another casino.

¹⁴ The term ‘casino chip’ also refers to plaques and other wagering instruments provided by the casino.

¹⁵ Ticket In/Ticket Out (TITO) is a gaming machine system that allows a gaming machine to accept either banknotes or tickets with a credit value printed on them (Ticket In) to commence play. TITO also prints tickets with a credit value when a player wishes to ‘cash out’ of the gaming machine (Ticket Out). The player can then redeem his/her ticket for cash at a cashier’s desk, ticket redemption kiosk, or insert the ticket into another TITO machine and continue playing. A ticket redemption kiosk machine is a multifunctional device, connected to a gateway or kiosk server, that can perform a variety of financial transactions for customers, such as redeeming slot machine/video lottery tickets for currency, exchanging currency for currency (*i.e.*, breaking bills or paper money), redeeming player slot club points, purchasing slot machine vouchers (*i.e.*, tickets), and initiating electronic transfers of money to or from a wagering account including currency withdrawals from a casino ATM.

89. The importance of studying money laundering methods – the “how to” – cannot be overstated. Such studies provide government decision-makers and operational experts with the material to target policies and strategies for combating financial crime. The sharing of these methods, together with indicators to detect money laundering activity, with responsible financial and non-financial organisations is equally important. They are a necessary tool for financial institutions, other financial intermediaries and gatekeepers who are on the front line in confronting activities that may or may not be suspicious (and thus may or may not be related in some way to money laundering, terrorist financing or some other financial crime).

90. For the private sector, and in this case casino owners and operators, valid money laundering indicators are therefore essential in establishing and “calibrating” mechanisms that help to identify suspicious or unusual transactions which must then be reported to a financial intelligence unit.

91. For the purposes of this chapter the following definitions apply:¹⁶

- *Method*: a particular procedure for carrying out money laundering activity. There are further distinctions in the concept of a money laundering method:
 - *Technique*: a particular action or way that the activity is carried out, for example, purchasing a cashier’s cheque.
 - *Mechanism*: a system or thing that carries out part of the process. An example of a money laundering mechanism is a casino.
 - *Instrument*: an object of value (or representing value) that is somehow used in the money laundering process, for example, a casino cheque or casino chips.

92. For example, the action of depositing funds into a casino account relates to all three concepts: *i)* depositing the funds is a *technique*, *ii)* the casino managing the account is a *mechanism* and *iii)* the funds deposited are an *instrument*. It should be noted as well that, for the most part, the examples provided for each of these concepts may not in and of themselves represent illegal activities. Indeed it is only when these *techniques*, *mechanisms* and *instruments* are put together to form a money laundering activity that they become illegal.

93. With regards to indicators, there is sometimes confusion between a money laundering indicator and a money laundering method. While it is sometimes true that the methods defined below could indicate money laundering activity, they are not synonymous. For example, exchanging chips for cash is not by itself an indicator of money laundering. By the same token, indicators are not all necessarily money laundering methods.

Criminal interest in casinos – players and infiltration of casinos

94. Casinos are attractive venues for criminals. Casinos are consistently targeted by criminals for criminal influence and criminal exploitation. Organised crime groups seek to control or own casinos or aspects of casino operations. Criminals attempt to infiltrate or influence casinos to facilitate theft, fraud, money laundering and other crimes.

95. A core function of all casino regulators is making certain that gaming is conducted honestly by approving the rules of the games and requiring the operator to provide a high standard of

¹⁶ Financial Action Task Force. *Money Laundering & Terrorist Financing Trends and Indicators Initial Perspectives*.

surveillance and security systems. This ensures public confidence in the gaming product, minimises opportunities for criminal activity and provides certainty of government revenue streams.

96. Criminal influence and exploitation of casinos appears to be both for possible money laundering, but also for recreation and in some cases enhancing their criminal endeavours outside the casino. Casinos have been noted as a place where criminals and organised crime figures like to socialise and particularly like to spend and launder their criminal proceeds.

97. Feedback from police also indicates that large casinos with sophisticated security and surveillance systems may be viewed by criminals as providing a safe haven to meet and associate in without fear for their personal safety.

98. Gaming venues attract ancillary criminal activities including loan sharking, vice and other crimes.

Box 4. Loan Sharking

Loan Sharking (also known as usury) is prevalent in casinos in a number of jurisdictions. Loan sharking is a crime that involves loaning money to individuals at an interest rate that is above a maximum legal rate, sometimes collected under blackmail or threats of violence. Loan sharks may be financed and supported by organised crime networks who are also involved in money laundering activities. A loan shark usually preys on individuals who are problem gamblers, struggling financially or, for some reason, are unwilling to seek credit from legal sources.

Persons in debt to loan sharks may be coerced into assisting with money laundering schemes in the casino.

Box 5. Credit card scam using the casino

A jurisdiction reported a credit card point scam where casino chips are purchased using credit cards. The chips are then cashed out and instead of crediting the credit card, casinos usually issue cash or a casino cheque. The balance on the credit card is eligible for consumer points. The balance on the credit card is paid back using the cash or cheque received from the casino. This method enabled large amounts of credit card points to be accumulated in a short period of time and can be used for merchandise purchases.

Money laundering methods and techniques in Casinos

99. The money laundering methods outlined in this chapter are:

- Use of Casino Value Instruments (cash / casino chips / TITO / gaming machine credits / cashier's orders / casino cheques / gift certificates / chip purchase vouchers / casino reward cards).
- Structuring / Refining.
- Use of Casino Accounts (credit accounts, markers¹⁷, foreign holding accounts) / facilities.
- Intentional losses.
- Winnings / intentional losses.

¹⁷ Casino markers act as a credit line through a personal checking account, no transaction occurs, but are issued once a patron submits their checking account number and a cheque to the casino. The casino has the right to deposit the marker at any time but usually waits a few months to allow for customers to pay back the credit if the losses are high. Money launderers will pay back the debt with the proceeds of crime.

- Currency Exchange.
- Employee Complicity.
- Credit Cards / Debit Cards.
- False Documents.

100. Each method is illustrated by representative cases¹⁸ and followed up with related indicators that can be used to detect suspicious or unusual transactions by casino owners and operators. The methods, cases and indicators have been generated from the following research material:¹⁹

- Sanitised case material from regulatory, law enforcement and security organisations.
- International case study and typology reports including FATF, APG and the Egmont Group.
- Open source research.

Casino value instruments

Cash / Casino Chips / TITO / Gaming Machine Credits / Cashier's Orders / Casino Cheques / Gift Certificates / Chip Purchase Vouchers / Casino Reward Cards

101. Casinos utilise various value instruments to facilitate gambling by their customers. The type and use of the value instruments listed above differs between casinos and is influenced by local regulation and casino operating structures. Casino value instruments are most often used for money laundering by converting illicit funds from one form to another.

102. Casino chips are the most common casino value instruments. Casino chips are issued by casinos and used in lieu of cash in gaming transactions between the house and players. Chips are round and marked with the denomination and name of the casino and are negotiable within the casino, or, in some cases, within casinos in the same group. Casinos may issue 'credit chips' which are different in colour and only used by patrons playing on credit. Casinos may issue 'dead chips' which are only used by *junket* patrons (*see section below on junkets*).

103. ***Buying chips for cash or on account, then redeeming value by way of a casino cheque, bank draft of money transfer.*** Launderers typically buy chips with cash or through their casino account. Chips bought on account may use a Chip Purchase Voucher (CPV) or similar value instrument. Repayment is then requested by a cheque, draft or transfer drawn on the casino's account. This method can be made more opaque by using a chain of casinos where the chips that were purchased with illicit cash are converted to credit, and transferred to another jurisdiction in which the casino chain has an establishment; the credit is then converted into in the form of a casino cheque at the second casino.

¹⁸ The cases outlined are provided from jurisdictions contributing to the project research, and while some countries may appear to be over/under-represented in the cases, this is not an indicator of high or low levels of money laundering within that country, but merely a reflection of that government's willingness to share money laundering information to support global AML awareness.

¹⁹ It is important to note that this chapter does not provide a description of all methods used to facilitate money laundering. It is limited to those methods that have been reported to FATF or APG and from cases that have been approved for use in the public forum.

104. Money launderers may hold the chips for a period of time, either using the chips to gamble in hopes of generating certifiable winnings or later redeeming the chips for cash/ cheque / transfer.

105. **Purchase of chips from ‘clean’ players at a higher price** – Money launderers may purchase chips from other money launderers or un-associated casino patrons with ‘clean’ backgrounds. This is done at a price greater than the chips’ face value. This is referred to as *value tampering*.

106. **Casino cheques payable to cash** – in some jurisdictions, casinos allow winning cheques to be made payable to ‘cash’. High-value casino cheques payable to cash have been observed in secondary circulation as bearer negotiable instruments and used as payment for goods or for reinvestment in criminal ventures, such as purchasing drugs. High-value casino cheques may originate from VIP rooms, which may provide alternative remittance services between player’s home jurisdictions and the casino VIP room.

107. **Combining winnings and cash into casino cheques** – although few jurisdictions allow this, money launderers seek to add cash to casino winnings and then exchange the combined cash and winnings for a single cheque.

108. **Use of chips as currency in illegal transactions** – money launderers may retain casino chips to be used as currency to purchase drugs or other illegal goods. Carrying chips from a drug transaction may also contribute to an alibi for the predicate offence. The recipient of the chips will later cash them at the casino.

109. Casino chips to be used as currency may be taken across borders and exchanged for payment of an illegal enterprise then returned by the third parties and cashed at the issuing or honouring casino in amounts below a reporting threshold. Most jurisdictions do not list casino chips as money value instruments and therefore do not require Customs declaration.

110. In some jurisdictions, casino chips from one casino can be utilised in another associated casino. Cases showed that the money launderers will take advantage of this arrangement to avoid attracting attention to their activities at the one casino. This may take in another jurisdiction. To prevent this some jurisdictions require casinos to have casino-specific chips and do not allow inter-casino chip cashing.

111. **Purchase of large numbers of ‘casino gift certificates’** – Cases have been detected of money launderers purchasing high value or numerous low value casino gift certificates which can be redeemed by 3rd parties. The certificates are then sold or given to other persons distancing the money launderer from the illicit funds.

112. **Purchase of casino reward cards** – Money launderers use illicit funds to purchase casino reward cards from legitimate customers paying them a premium above the value of the reward.

Case 1. Casino used as preferred method to launder millions

Offence:	Money Laundering
Jurisdiction:	Australia
Technique:	Chip purchase and cash out, claiming credits as jackpot wins, playing games with low return and high win.
Mechanism:	Casino
Instrument:	Casino chips, casino cheques

Information identified alleged money launderers using the casino as a preferred method of laundering millions of dollars accumulated from criminal activities. The methods used to launder the money included purchasing and cashing out chips without playing, putting funds through slot machines and claiming credits as a jackpot win and playing games with low returns but higher chances of winning. The same group were also utilising bank

accounts and businesses to launder funds.

Case 2. Purchase of chips and gambling without clear intention to win

Offence:	Money Laundering
Jurisdiction:	Belgium
Technique:	Chip purchase and cash out, claiming credits as jackpot wins, playing games with low return and high win.
Mechanism:	Casino
Instrument:	Casino chips, casino cheques

Two Asian males residing in Belgium went to a Belgian casino twice to purchase chips for a total amount of almost 25 000 EUR. When visiting they did not play at the tables and immediately collected funds through a third person, also an Asian national.

Investigations indicated that the three persons were students and lived at a common address with other Asian students. It appeared that the transactions were likely to be linked to human trafficking. By not playing at the casino and collecting the money through a third person they wanted to leave a paper trail in order to justify the origin of the funds.

Case 3. Proceeds of drugs used to purchase chips and claim funds as winnings

Offence:	Drug importation
Jurisdiction:	Australia
Technique:	Chip purchase and cash out
Mechanism:	Casino
Instrument:	Casino chips, chip to cash transfer, casino cheques

A cargo consignment addressed to a person contained approximately 3.4 kilograms of black opium resin, concealed within the contents. The person was arrested when attempting to collect the consignment. Further investigation revealed the person to be a regular customer of a casino, having conducted approximately 50 betting transactions, predominantly chip cash outs totalling AUD 890 000. Very little casino gaming play was recorded for the person and it was assumed that he used the proceeds from previous importations to purchase chips and claim the funds as winnings.

Case 4. Proceeds from stolen cheques used to purchase casino chips

Offence:	Money Laundering
Jurisdiction:	United Kingdom, India
Technique:	Purchase casino chips
Mechanism:	Casino
Instrument:	Casino chips

In November 2007 two men were convicted for their part in a GBP 25 000 cheque scam. The victim was robbed at New Delhi Railway Station in India in March 2006 and among the items stolen were two Barclays cheque books. The money laundering trail led authorities to a casino in London where cash withdrawn from the defendants account was used to purchase gambling chips. Both men claimed gambling addictions. STRs were not submitted by the casino in this case.

Case 5. Cash laundered through casino used to bribe officials

Offence:	Money Laundering
Jurisdiction:	Korea
Technique:	Cash to chip to cash/cheque transfers
Mechanism:	Casino
Instrument:	Casino chips, casino cheques

Early 2006 a bribery case involving money laundering at a casino was investigated by the Public Prosecutor's Office. A legal broker bought casino chips with cheques to a total of KRW 20 billion (approx USD 20 million) from 2003 to 2005 and then changed the chips with cash and cheques issued by the casino. He then used the money to bribe politicians and senior government officials.

Case 6. Casino reward cards traded for gold coins

Offence:	Money Laundering
Jurisdiction:	United States
Technique:	Purchase casino reward cards from legitimate customers
Mechanism:	Casino
Instrument:	Casino reward cards, gold coins

A suspect purchased casino reward cards from legitimate customers at a US casino. The cards increase in value with each casino visit and with each gambling session. The cards were purchased with illicit funds and were then traded for gold coins at the casino's store. An employee at the store was an accomplice in the laundering scheme.

Case 7. Embezzled money laundered through casino

Offence:	Money Laundering
Jurisdiction:	United States
Technique:	Purchase and cash out with little or no gaming activity
Mechanism:	Casino
Instrument:	Casino chips

A lawyer was sentenced in New Jersey for embezzling more than USD 500 000 and laundering USD 250 000 of it through an Atlantic City casino. The defendant wire transferred USD 250 000 to the casino and arrived at the casino later the same day to launder the funds. He purchased casino chips and gambled for an hour on a roulette table losing USD 10 000. He then cashed out the remaining USD 240 000 into currency and left the casino.

Case 8. Embezzled money laundered through casino

Offence:	Money Laundering
Jurisdiction:	Spain
Technique:	Purchase and cash out with little or no gaming activity, casino cheques in the name of 3rd parties
Mechanism:	Casino
Instrument:	Casino chips

Different people entered separately in a casino and bought chips. After playing minor amounts of chips they tried to change chips and requested a cheque paid to the name of a third person. They tried to do the same operation with different people and lower amounts one day later, which raised suspicion of casino operators.

Indicators of ML using casino value instruments

- Inserting funds into gaming machines and immediately claiming those funds as credits.
- Customers claiming gaming machine credits/payouts with no jackpot.
- Customers claiming a high level of gaming machine payouts.
- Noticeable spending/betting pattern changes.
- Customers frequently inserting substantial amounts of banknotes in gaming machines that have high payout percentages and do not play "max bet" to limit chances of significant losses or wins, thereby accumulating gaming credits with minimal play.
- Frequent even-money wagering when conducted by a pair of betters covering both sides of an even bet (e.g., in roulette, baccarat/mini-baccarat, or craps).
- Customer's intention to win is absent or secondary.

- Two or more customers frequently wagering against one another on even-money games.
- Customer in possession of large amounts of coinage or bills.
- Customer befriending/attempting to befriend casino employees.
- Purchasing and cashing out casino chips with little or no gaming activity.
- Customer requests to add cash to casino winnings and then exchanging the combined cash and winnings for a single cheque.
- Multiple cheques being requested or drawn on account.
- High volume of transactions within a short period.
- Multiple chip cash outs on the same day.
- Structuring of chip/cheque transactions.
- Chip cash out is same/similar to chip purchase.
- Requests for credit transfers to other casinos.
- Use of multiple names to conduct similar activity.
- Use of third parties to purchase casino chips.
- Use of credit cards to purchase casino chips.
- Use of personal cheques, bank cheques and traveller's cheques to purchase casino chips.
- Customer due diligence challenges, e.g. refusals, false documents, one-offs, tourists passing trade.
- Customer purchases chips and leaves casino shortly after.
- CPV, TITO, ticket or voucher dated prior to date of redemption.
- Large chip purchases.
- Frequent purchase of casino gift certificates.
- Unexplained income inconsistent with financial situation/customer profile.
- Supposed winnings do not correspond with recorded winnings.
- Dramatic or rapid increase in size and frequency of transactions for regular account holder.
- Detection of chips brought into the casino.

Structuring

113. Structuring or ‘smurfing’ involves the distribution of a large amount of cash into a number of smaller transactions in order to minimise suspicion and evade threshold reporting requirements. Common methods of structuring include:

- Regularly depositing or transacting similar amounts of cash, which are below a country’s reporting disclosure limit
- The use of third parties to undertake transactions using single or multiple accounts.
- Using cheques from multiple financial institutions or branches of a financial institution to ‘buy in’ while the amount of each cheque is below the reporting threshold.
- Utilising shift changes to systematically ‘cash in’ chips or other value instruments to avoid threshold reporting.
- Regularly switching gaming tables, gaming rooms, junkets or casinos within a chain when the wagering amounts are approaching the reporting threshold.
- Requesting the division of winnings or prize money, which exceeds the reporting threshold, to be broken down into cash and chips below the reporting threshold in order to exchange it at the cashier’s desk.

114. While money launderers will often structure their transactions to avoid financial institutions filing reports to authorities, it has been found that some money launderers using casinos have the opposite strategy and seek to trigger a cash transaction report to further authenticate a transaction.

Case 9. Using reporting thresholds to legitimise suspicious transactions

Offence:	Money laundering
Jurisdiction:	United States
Technique:	Use of third parties, triggering transaction reports to legitimise suspicious transactions
Mechanism:	Casino
Instrument:	Casino chips, casino cheque

A number of persons purchased chips with illicit cash in amounts below the CTR threshold, but then passed the chips to one individual who cashed out, receiving a casino cheque and triggering the filing or a CTRC that gave the appearance of further authenticating the transaction. Over a twelve-month period, one individual was named in casino CTRCs reporting UDS1.1million paid out, but was not named in a single CTRC for cash taken in.

Refining

Exchanging low denomination for high denomination currency

115. Individual launderers or organised groups use casino services to refine large amounts of low denomination bank notes into more manageable high denomination notes. Some countries note this as being associated with drug dealers who accumulate large amounts of small denomination bills from drug sales. In cases of groups, they may seek to refine money by dividing it amongst the group before entering the casino. The group enter the casino, individually refine their portion of the money and meet again outside the casino to assemble the total amount. The refining techniques most commonly identified are listed below:

116. ***Refining using the cashier's desk*** – money launders exchange coins or small denomination bills for larger denomination bills at the cashier's desk.

117. ***Refining using 'note acceptors' or gaming machines that accept cash*** – Most casinos with gaming machines have 'note acceptors'. Money launderers will feed currency notes into the machine to accumulate credit with little or no play before redeeming the credits. As the amount can be quite large, it requires a 'ticket' or similar document provided by the slot attendant as proof to enable the exchange for cash or cheque at the casino cashier's desk. Gaming machines, Video Lottery Terminals (VLTs) and Ticket In/ Ticket Out (TITO) machines are used to refine currency. Gaming machines, TITO machines and VLTs are fed large sums of low denomination cash. Launderers redeem credits with minimal play. The ticket is then cashed at the cashier's desk, ticket redemption kiosk, for high denomination bills.

118. ***Use of casino account for refining*** – launderers pay low denomination cash into their casino accounts and withdrawn funds with cash of higher denominations.

Case 10. Refining low denomination notes

Jurisdiction:	Spain
Technique:	Refining, Use of third parties
Mechanism:	Casino
Instrument:	Cash, casino chips, remittance arrangement

A group of three foreign people entered separately in a casino and bought chips, paying with low denomination notes. They didn't play any game, and after they changed the chips that they had bought trying to obtain high denomination notes.

Case 11. Drug proceeds converted into casino chips by third parties

Offence:	Drug importation
Jurisdiction:	Australia, Vietnam
Technique:	Use of third parties
Mechanism:	Casino, remittance agent
Instrument:	Casino chips, remittance arrangement

A person was involved in the importation and distribution of heroin into Australia from Vietnam. The person gambled a large proportion of the proceeds at casinos and used third parties to purchase gaming chips on his behalf. Reports from the casino noted multiple chip cash outs on the same day, with some of these transactions being structured to avoid the AUD 10 000 reporting threshold.

Further investigations noted that he would send large cash payments to various entities in Vietnam through a remittance dealer. The remittance dealer was a trusted associate of the person and had been non-compliant with his reporting obligations.

Indicators of ML using structuring/refining methods

- Activity was inconsistent with the customer's profile.
- Associations with multiple accounts under multiple names.
- Use of multiple names to conduct similar activity.
- Depositing multiple amounts of cash and receiving multiple cheques drawn on that account.
- Multiple individuals sending funds to the one beneficiary.
- Cheque issued to a family member of the person.

- Third party presents for all transactions but does not participate in the actual transaction.
- Transferring funds into third party accounts.
- Transactions on casino accounts conducted by persons other than the account holder.
- Use of third parties to undertake structuring of deposits and wire transfers.
- Use of a remittance dealer / junket operators to deposit or withdraw cash.
- Use of third parties to purchase gaming chips.
- Use of third party to conduct wagering.
- Cash handed to third party after cash out.
- High volume of transactions within a short period.
- Purchasing and cashing out casino chips with no gaming activity.
- Exchanging large quantities of quarters from non-gaming proceeds for paper currency.
- Frequent betting transactions just under thresholds.
- Frequent 'buy in' and 'cash out' transactions just under thresholds.
- Cash deposits / withdrawals just under thresholds.
- Wire transfers / currency exchanges just under thresholds.
- Requests for winnings in separate cash or chip amounts under reporting threshold.
- Cashing in winnings in a multiple combination of chips, cheque and cash.
- Customer conducts several transactions under reporting thresholds over several shift changes.
- Customer moving from table to table or room to room before the wagering amounts reach the reporting threshold.
- Opening a casino account or purchasing casino chips with small denominations bills.
- Customer gambling with large amounts of small denomination bills.
- Currency exchange from small denomination bills to larger denomination bills.
- Frequent 'cash out' transactions without corresponding 'buy in' transactions or vice versa.
- Customer due diligence challenges, e.g. refusal, false documents, one-off/tourist or passing trade.
- Dramatic or rapid increase in frequency of currency transactions for regular account holders.
- Noticeable spending/betting pattern changes.

- Insert banknotes in electronic gaming devices with no gaming activity, press the “cash out” button which generates a TITO ticket, and redeem ticket at cashier’s desk or ticket redemption kiosk machine.

Casino accounts & facilities

Credit accounts / Markers / Foreign holding accounts / safe deposit boxes

119. Casino accounts provide criminals further opportunities to attempt to laundering crime proceeds. Many casinos offer deposit accounts and lines of credit with less scrutiny and CDD requirements than financial institutions. The frequent movement of funds between financial institutions and casinos, or between casino accounts held in different casinos may be vulnerable for money laundering. Many casinos offer private safe deposit boxes, particularly to VIP/’high roller’ customers.

120. ***Cashing cheques into casino accounts*** – Some casinos allow customers to cash various types of cheques and use the proceeds for gambling. Cheques could be signed over to the bearer by the cheque recipient. In the cases studied, proceeds from illegal activity were initially used to draw these cheques with the aim of avoiding the casino’s suspicion.

121. ***Deposits into casino accounts by wire transfers or bank cashier’s cheque*** – funds are deposited by wire transfer of bank cheque, then cashed out or moved to other accounts with minimal or no gambling activity.

122. Cashed out funds are stored in casino safety deposit boxes or held in the form of safekeeping markers and then cashed out.

123. ***Foreign Holding Accounts (FHAs)*** – Accounts that are held in one jurisdiction by the casino, but the funds can be used to gamble in another jurisdiction under the same casino group. For example, funds held in a FHA account in Macao, China can be used to gamble at a casino in Las Vegas. The money held in the account does not physically leave the country and is not subject to cash declarations. Large casinos may operate marketing offices in jurisdictions other than where the casino is located. Patrons are able to pay in funds to their casino account to be played when they travel to the casino without sending a cross-border wire transfer. *See the Junkets section for further details.*

124. ***Wire transfers from Casas de Cambio to casino accounts*** – Casas de Cambio in another jurisdiction may wire transfer funds to casinos. As an example, in the United States Casas de Cambio businesses are concentrated along the southwest border, with over 1 000 located along the border from California to Texas. These businesses are generally unregistered and do not comply with AML reporting requirements, and are suspected of being a significant money laundering risk. These *Casas de Cambio* have corresponding bank accounts which allow them wire transfer of large amounts of cash to casinos and other institutions throughout the world.

125. ***Safety deposit boxes*** – A number of casinos offer safety deposit boxes to patrons, in particular to ‘high roller’ patrons in VIP rooms. These present a risk due to the lack of transparency with the use of such boxes and the possibility for 3rd parties to be given access to safety deposit boxes via a password or key, to facilitate financial transactions. Very few jurisdictions regulate the safety deposit boxes in casinos.

Case 11. Large money laundering conspiracy

Offence:	Money laundering, VAT fraud, counterfeiting, credit card fraud, drug trafficking
Jurisdiction:	United Kingdom, Dubai
Technique:	Use of casino accounts, placement via gambling
Mechanism:	Bank, casino
Instrument:	Cash

The money laundering conspiracy involved millions of UK pounds from organised criminal gangs being laundered by a group of men from West Midlands. The money laundered included the profits from a number of activities including drug trafficking, multi-million pound VAT conspiracies in the mobile phone industry, counterfeiting and credit card fraud. The monies were a mixture of Scottish and English notes. The defendants would transfer large amounts of money to a bank account in Dubai, which would then be accessed by their associates. The defendants received the proceeds of crime in the UK and made equivalent amounts of criminal monies available in Dubai. They then utilised the gambling industry to launder the money. Money was placed on a deposit at a casino and withdrawn a day or so later. Other sums would be gambled. Thousands of pounds would be passed over the tables in order to disguise the original source of the banknotes. Monies gambled or exchanged at the casino provided the defendants with an apparently legitimate explanation as to their source.

Case 12. Bank employee gambles millions from clients' accounts

Offence:	Fraud, money laundering
Jurisdiction:	Australia
Technique:	Use of casino accounts, structuring
Mechanism:	Bank, casino
Instrument:	Bank cheques

An investigation into a bank employee who gambled millions of dollars from clients' accounts was initiated as a direct result of information submitted by the casino. The suspect used his knowledge of the bank's internal procedures to discreetly transfer funds from customer accounts to his own personal account. Over a period of time, these funds were deposited into his casino account in the form of bank cheques made out in his name. The casino reported the regular deposit of bank cheques. The same casino had also previously reported bets placed by the suspect of AUD 9 000 to avoid the AUD 10 000 reporting threshold. As a result of the investigation the suspect was charged with three counts of money laundering and 37 counts of fraud.

Case 13. Avoiding liquidation action

Offence:	Money laundering
Jurisdiction:	Australia
Technique:	Placement via gambling
Mechanism:	Casino
Instrument:	Cash

A person was a director of a company that was subject to liquidation. Contrary to liquidator's instructions, the person began transferring large amounts of cash between company accounts and depositing the money into a casino account. The funds were used to gamble at the casino and subsequent "winnings" taken as cash.

Case 14. Cigarette Fraud

Offence:	Money laundering, bank fraud, wire fraud, conspiracy
Jurisdiction:	United States
Technique:	Use of third parties and casino accounts to facilitate fraud
Mechanism:	Casino
Instrument:	Cash, Casino Cheques

A suspect in New York lured foreign buyers into ordering large quantities of cigarettes. Suspect did not have cigarettes and had no intention of providing them to the buyers. The casino was used to launder the funds from the fraud as below:

- Buyer 1 paid USD 100 000 up front in a casino cashier's cheque. Suspect had accomplice deposit the cheque at the casino. Accomplice was permitted to gamble with USD 10 000 and cash out remainder and give to suspect.
- Buyer 2 provided a USD 60 000 certified cheque up front. Accomplice deposited the cheque at the same casino and was permitted to gamble, but lost USD 50 000 and gave remaining USD 10 000 in cash to

defendant. Buyer 2 sent another USD 100 000 certified cheque.

- Buyer 3 deposited USD 600 000 cheque into an account against which a cheque in the amount of USD 180 000 was made payable to the same casino. Accomplice then tried to withdraw all of the money, but the casino refused and permitted only a USD 50 000 withdraw. Accomplice then gambled with some funds and won USD 15 000. Casino then permitted withdrawal of funds and allowed accomplice to cash out.

Case 15. Loan-sharking profits laundered at casino

Offence:	Money laundering
Jurisdiction:	Japan, United States
Technique:	Purchase and cash out with little or no gaming activity
Mechanism:	Casino
Instrument:	Cash, casino chips, casino credit

A boss of a loan-shark business ordered his associates to convert the profits from Yen into US currency using false names. These funds were then distributed to numerous bank accounts around the world. Some of the money was also invested with a foreign agent of a Las Vegas casino, who kept the money in a safety deposit box in the head office of a major Tokyo bank. Against the security of this money, the boss played frequently at Las Vegas casinos as a VIP player. Although he gambled in the VIP room, he would never place big bets and, after minimal play, would frequently cash in his chips for US currency. His associated were also circulated through a number of Las Vegas casinos cashing in chips worth USD 2 000 or less.

Indicators of ML using casino accounts:

- Frequent deposits of cash, cheques, bank cheques, wire transfers into casino account.
- Funds withdrawn from account shortly after being deposited.
- Significant account activity within a short period of time.
- Account activity with little or no gambling activity.
- Casino account transactions conducted by persons other than the account holder.
- Funds credited into account from country of concern.
- Large amounts of cash deposited from unexplained sources.
- Associations with multiple accounts under multiple names.
- Transfer of funds from/to a foreign casino/bank account.
- Transfer of funds into third party accounts.
- Funds transferred from casino account to a charity fund.
- Multiple individuals transferring funds to a single beneficiary.
- Structuring of deposits / withdrawals or wire transfers.
- Using third parties to undertake wire transfers and structuring of deposits.
- Use of an intermediary to make large cash deposits.

- Use of gatekeepers, e.g. accountants and lawyers to undertake transactions.
- Use of multiple names to conduct similar activity.
- Use of casino account as a savings account.
- Activity is inconsistent with the customer's profile.
- Unexplained income inconsistent with financial situation.
- Transfers with no apparent business or lawful purpose.
- Transfer of company accounts to casino accounts.
- Use of false and stolen identities to open and operate casino accounts.
- Customer name and name of account do not match.
- U-turn transactions occurring with funds being transferred out of country and then portions of those funds being returned.
- Customer due diligence challenges, e.g. refusal, false documents, one-off/tourist or passing trade.
- Requests for casino accounts from Politically Exposed Persons (PEPs).

Winnings

126. ***Use of illicit funds to gamble*** – this is the simplest method of gambling illicit funds in the home hopes of generating certifiable winnings. One way to do this is to play gaming machines or other games with low payout higher win/loss ratios. The money launderer will then receive a casino cheque for the total amount of credits remaining on the machine plus the jackpot.

127. Some jurisdictions require casinos to endorse the casino cheques from jackpots as 'winnings' in order to differentiate it from a cheque generated as a result of cashing out large amounts of machine credits.

128. ***Buying winnings from legitimate customers*** - is another method used across the gaming sector. Money launderers will approach customers and offer them cash at a premium above their winnings. This was evident with customers who had won gaming machine jackpots, or accumulated a large amount in casino chips from winnings on table games, or customers that had won in other forms of betting offered by some casinos, such as electronic lotteries, horse racing and sports betting.

129. ***Parallel Even money betting*** – In cases where gambling is undertaken to launder funds, it is usually on low odds, low risk games such as the even money options on roulette. This would involve two or more persons placing opposite equivalent bets on even money wagers in the same game. As an example Person A places USD 1 400 on red, while Person B places USD 1 400 on black in a game of roulette. The bet is 'double or nothing'. In this case the winning party would win just under USD 3 000 which could be paid out with a 'winnings' cheque and the size of the win would not trigger CDD requirements at the roulette table.

130. ***Betting against associates / intentional losses*** – This is also the case in games where which provide money launderers the option to bet against an associate so that in most cases one party will win. These ‘intentional losses’ where money launderers are intentionally losing to one of the party, who is able to receive a casino issued cheque or wire transfer of ‘legitimate’ winnings.

Case 16. Overseas nationals purchase winning jackpots with illegal proceeds

Offence:	Drug trafficking & money laundering
Jurisdiction:	Spain
Technique:	Buying winning lottery tickets
Mechanism:	Lotteries
Instrument:	Winning jackpots, cash

Investigations in Spain related, mainly with drug trafficking, corruption and tax fraud identified the use of gaming to launder funds. The technique consisted of buying winning lottery tickets from legitimate gamblers.

Case 17. Overseas nationals purchase winning jackpots with illegal proceeds

Offence:	Money Laundering
Jurisdiction:	Australia
Technique:	Buying winning jackpots
Mechanism:	Gambling clubs
Instrument:	Winning jackpots, casino cheques

A group of overseas nationals were identified buying winning jackpots from other persons at various clubs in Sydney, Australia. The suspects deposited approximately AUD 1.7 million in winning cheques within a year, immediately withdrawing money in cash afterwards. The source of the funds used to buy winning jackpots was suspected to be from illegal means.

Indicators of ML using winnings:

- Frequent claims for winning jackpots.
- Frequent deposits of winning gambling cheques followed by immediate withdrawal of funds in cash.
- Customers watching/hanging around jackpots sites but not participating in gambling.
- Multiple chip cash outs on the same day.
- Customers claiming gaming machine credits/payouts with no jackpot.
- Customers claiming a high level of gaming machine payouts.
- Purchasing and cashing out casino chips with no gaming activity.
- Requests for winnings in separate cash or chip amounts under reporting threshold.
- Frequent ‘cash out’ transactions without corresponding ‘buy in’ transactions.
- Cashing in winnings in a multiple combination of chips, cheque and cash.

Currency exchange

131. Given the popularity of casino-based tourism and the willingness of customers to travel to legal casino sectors, most casinos offer currency exchange services.

132. **Conversion of large sums of foreign currency** – launderers may use large, one-off, or frequent foreign currency exchanges or deposits of a foreign currency. This may not appear suspicious in jurisdictions with high numbers of foreign players.

133. Reported cases indicate that criminals involved in the distribution and supply illegal drugs are using casino currency exchange services to convert their criminal proceeds from one currency to another, in order to alter its original form.

134. Individuals and groups will also employ structuring methods to undertake currency exchanges without triggering threshold reports. They will use multiple casino locations and once the currencies are exchanged, will meet again to assemble the total amount.

135. **Casino play is undertaken in foreign currency** – in some poorly regulated jurisdiction, customers are able to purchase chips directly in a foreign currency (for example in Nepal with USD and Indian Rupees).

Case 18. Overseas nationals purchase winning jackpots with illegal proceeds

Offence:	Money Laundering
Jurisdiction:	Spain
Technique:	Currency conversion
Mechanism:	Casino
Instrument:	Cash – various currencies

A group of foreign people entered separately in a casino to buy casino chips using Swiss Francs (CHF). The purpose of the syndicate was not to play in the casino, but to redeem the chips in Euros. The casino detected the operations, stopped the transactions and filed an STR.

Indicators of ML using currency exchange:

- Bank drafts/cheques cashed in for foreign currency, e.g. Euros, USD.
- Multiple currency exchanges.
- Dramatic or rapid increases in size and frequency of currency exchange transactions for regular account holders.
- Currency exchange for no reasonable purpose.
- Currency exchanges with low denomination bills for high denomination bills.
- Currency exchanges carried out by third parties.
- Large, one-off, or frequent currency exchanges for customers not known to the casino.
- Requests for casino cheques from foreign currency.
- Currency exchanges with little or no gambling activity.

- Structured currency exchanges.

Employee complicity

136. Employee complicity is another method in which third parties are used to facilitate money laundering. Individual employees or organised groups comprising of staff from different departments conspire with customers to enable money laundering transactions to go undetected. Methods include:

- Failing to file suspicious transaction reports or threshold transaction reports.
- Destroying documents/transactions reports related to due diligence or reporting processes.
- Falsifying player ratings and other gambling records to justify the accumulation of casino chips/gaming machine credits.

137. Some jurisdictions have raised vulnerabilities from providers of gaming equipment and machines as well as contractors that supply goods with a potential to impact on the integrity of the operation. Major contracts can be an avenue for criminal exploitation of the operation (*e.g.* through corrupt purchasing and under supply of contract goods). Criminals will try to exploit gaming equipment and associated computer systems to achieve theft and money laundering in the casino.

Case 19. Suspected falsified player ratings

Offence:	Money laundering
Jurisdiction:	Australia
Technique:	Falsifying player ratings to legitimise criminal proceeds
Mechanism:	Casino
Instrument:	Cash

An ex-employee of one casino was investigated by Australian authorities after he was able to purchase a house for cash. The family of this person is alleged to be involved in illegal drug activity and it was suspected that the funds used to purchase the house were provided by his family. The person, however, was able to show 'player ratings' from a second casino to show how he had turned NZD 20 000 into over NZD 400 000 in two weeks. It is suspected that an accomplice at the second casino falsified these 'player ratings', but this was not able to be proven.

Case 20. Back door corruption

Offence:	Money laundering
Jurisdiction:	United States (Indian casino)
Technique:	Casino staff bribed to facilitate money laundering
Mechanism:	Casino
Instrument:	Cash, jackpots

In Florida drug proceeds were laundered through gaming machines. Some gaming machines are controlled by software that have certain override features, or 'back doors' that give key casino staff the ability to force jackpot payouts. In Florida drug dealers bribed casino staff who accessed the override features and rigged a number of machines for the drug dealers to play and win jackpots from their drug proceeds.

Indicators of employee complicity:

- Contact between patrons and casino staff outside of the casino.
- Supposed winnings do not correspond with recorded winnings.

- Dramatic or rapid increases in size and frequency of currency transactions for regular account holders.
- Large sums of cash from unexplained sources.
- Large sums credited into accounts from other jurisdictions or countries of concern.²⁰
- Associations with multiple accounts under multiple names.
- Transactions on casino accounts conducted by persons other than the account holder.
- Deposits into casino account using multiple methods.
- Cheques issued to a family member of the person.
- Multiple individuals sending funds to a single beneficiary.
- Third party presents for all transactions but does not participate in the actual transaction.
- Transferring funds into third party accounts.
- Use or third parties to undertake wire transfers.
- Use of an intermediary to make large cash deposits.
- Use of gatekeepers, e.g. accountants and lawyers to undertake transactions
- U-turn transactions occurring with funds being transferred out of a country and then portions of those funds being returned.
- Use of remittance agents to move funds across borders.
- Use of third parties to purchase gaming chips.
- Use of third party to conduct wagering.
- Wire transfers from third parties in tax haven countries.
- Junket tours where funds can be concealed amongst the pool for the group.
- Cash handed to third party after cash out.

Credit cards / debit cards

138. ***Laundering proceeds from stolen credit cards*** – Casinos in some jurisdictions allow customers to purchase casino chips using credit cards. In cases where the cards are not stolen or fraudulently obtained, the outstanding credit card balances are paid by the card holder at the bank using the illicit funds.

20. TBD.

139. **Credit cards** – criminals use of credit cards provides an opportunity for authorities to follow the money trail more readily.

Case 21. Debit card scheme

Offence:	Fraud, money laundering
Jurisdiction:	Belgium
Technique:	Use of credit cards to conduct money laundering transactions
Mechanism:	Casino
Instrument:	Credit cards, casino chips.

A person residing in Belgium, originally from Eastern Europe, visited a casino on the Belgian coast on two occasions and bought gaming chips for a total value of EUR 400 000 paid for in cash and with credit cards. The casino reported these transactions to the FIU.

Based on the history of gambler's purchases using credit cards it was determined that his account had been extremely active: it had been inundated with various transfers from companies and, in particular, with many cash deposits. The spouse of the party concerned ran a business in Belgium and maintained underworld links with organised crime from Central and Eastern Europe. The party concerned received citizens from those countries at his personal address and that financial transactions were carried out in cash. The gambler was in frequent contact with a person who was being investigated for the laundering of money deriving from organised crime.

140. **Debit cards** – are another value instrument used to conduct fraud and money laundering crimes. In the case below, criminals would join a casino and use their debit card to draw up to the casino's maximum standard daily limit and purchase casino chips. The subjects either do not put any funds at risk or there would be minimal play. The subjects would then typically cash out. In similar cases, plaques would be passed to an associate for play. Sometimes all the funds would be put at risk. The major operators quickly identified this trend and put risk control mechanisms in place to limit the initial debit card transaction to a much lower limit for first time transactions in high risk situations.

Case 22. Debit card scheme

Offence:	Fraud, money laundering
Jurisdiction:	United Kingdom
Technique:	Use of debit cards to conduct money laundering transactions
Mechanism:	Casino
Instrument:	Casino plaques

An existing member of a casino introduced a number of people over a period of time. Suspicious was raised as the new members were completing debit card transactions to the maximum limit and receiving gaming plaques in exchange, which in turn were passed to the existing member. Most of the new members never returned to the casino after the initial visit. The nationalities of the new members varied widely, but all are believed to have recently arrived from foreign jurisdictions. The transactions varied from GBP 1 000 to 7 000. Some money was put at risk and lost by the existing main member.

Indicators of ML using credit/debit cards:

- Purchasing casino chips using credit card.
- Purchasing casino chips using debit card.
- Purchasing and cashing out casino chips/plaques with no gaming activity.
- Customer purchases chips and leaves casino shortly after.
- Use of stolen or fraudulently obtained credit card.

- Use of multiple credit/debit cards to purchase casino chips.
- Use of third parties to purchase chips using credit/debit card.
- Structuring of credit card transactions.
- Conducting debit card transactions up to the maximum limit.
- Chip cash out is same/similar to chip purchase.
- Customer due diligence challenges, e.g. refusals, false documents, one-offs, tourists passing trade.

False documents

141. As with financial institutions, money launderers use false documentation to disguise the origin of criminal proceeds and to protect the identity of those laundering the proceeds.

142. **False identification documents** – often used to conduct financial transactions at the casino, open casino accounts, undertake gambling transactions and redeem winnings.

Case 23. Money launderer uses third parties and false identities to launder drug proceeds

Offence:	Money laundering, identity fraud
Jurisdiction:	United States
Technique:	Use of 3rd parties and false identities to structure gambling transactions
Mechanism:	Casino
Instrument:	Cash, casino chips

A Person of Interest (POI) of a drug trafficking organisation, utilising both the money he was paid for his services and the large sums of money put into his possession to be laundered, elevated his previously modest gambling practices to that of a high-roller. The person would recruit third parties at the casino to purchase, or cash in, chips for him, paying them a nominal fee to do so. After gambling, he would cash some of these third-party purchased chips back out again, claiming they were his gambling winnings. According to the CTRs a USD 313 000 discrepancy was found to exist between chip purchases and cash out. Twenty-four of the CTRCs recording his activities revealed the use of aliases and multiple social security numbers. On numerous other CTRCs he had refused to provide a social security number.

Indicators of ML using false documents and counterfeit currency:

- Associations with multiple accounts under multiple names.
- Purchasing chips or undertaking cash transaction and immediately leaves casino.
- Transferring funds into third party accounts.
- Use of multiple names to conduct similar activity.
- Use of altered/fraudulent or stolen identification to conceal identity.
- Customer due diligence challenges, e.g. refusal, false documents, one-off/tourist or passing trade.

- Inconsistent identity information presented.
- Refusal to provide identification / false identification or Social Security numbers.
- Using false or multiple Social Security numbers.
- Refusing to provide required identification.

CHAPTER 3 – SECTOR VULNERABILITIES AND EMERGING ISSUES

Introduction

143. This chapter identifies some of the sector vulnerabilities and emerging issues within the global casino sector, as reported by members of the FATF, APG and other FATF-style regional bodies (FSRBs).

Casino-based Tourism – “Junkets”

144. Casino junkets or casino-based gaming tours are derived from casino marketing programs. A junket is an organised gaming tour for people who travel to the casino primarily to gamble. The junket may include transport, accommodation, incentives to play at the casino and the movement of funds to and from the casino.

145. Casino junkets may be part of the casino’s in-house marketing operation or may be run by independent operators who have a contract with the casino. In jurisdictions where the role of junkets is limited, they may still operate in travel agent roles with an added service of moving funds to the jurisdiction. In such cases, junkets may have no direct connection to the casino, but just bring the players and their funds to the front door of the casino. Junket agents are persons or companies who have a role to sign up casino patrons to take part in junkets. Junket representatives work to organise the junket.

146. In house marketing by casinos may include representative offices of the casino being located in foreign jurisdictions in order to organise junket gaming tours to the casino jurisdiction.

147. Junkets appear to be common in casino jurisdictions in the Americas, Caribbean and Asia, but are less common in European casinos. The extent of junket operations in casinos in Africa, the Middle East and Central Asia is unclear.

Regional junket patterns

148. A number of casino sectors in the Asia/Pacific region have a sizable junket industry to attract gambling tourists to their sector. As at 28 January 2009 Macao, China has 153 licensed junket operators, made up of 107 companies and 46 individuals. The patterns of casino-based tourism in the Asia Pacific region vary but source jurisdictions include China, India, Hong Kong, Japan, Chinese Taipei, Thailand, Australia, New Zealand and the United States.

149. Junkets do not operate in Canada and it is reported that junkets do not operate in much of Europe, although Malta reported EUR 28 million in revenues from junkets operations in 2006 and Austria reports that there is only small-scale activity in the sector, due to tight regulations applicable to casino customers. While casino-linked junkets are not a feature of some casino sectors in Europe, it is likely that junkets are a relatively recent development for this region and authorities may not yet recognise junket-type operations or the level of risk they present.

Features of Junkets

150. Junket operators provide incentives for patrons to play at a particular casino. As part of this, the junket provider may organise all aspects of a player's tour to the casino, including the movement of funds to be played in the casino. Junkets generally target the high net worth clients. In some jurisdictions, junket operators and their agents have a role in conducting CDD on junket patrons.

151. In house marketing by casinos may include representative offices of the casino being located in foreign jurisdictions in order to organise gaming tours to the casino jurisdiction. In such cases, players can organise all aspects of their visit to the casino, including depositing funds into their casino account. An example is Wynn Resorts, which has casinos in Las Vegas and Macau and has marketing executives located in local offices in, Tokyo, Hong Kong, Singapore, Taipei and Vancouver. Other large-scale casinos operate similar networks of offices.

152. Junket representatives / agents serve as an agent between casino marketing departments and proven premium players. VIP junkets do not tend to be advertised. Region specific junkets often do not deal with the general public, but rely on introductions from intermediaries. Junket representatives / agents rely on commissions or fees to support their business. These commissions vary, but may include:

- A percentage of front money.
- A commission on 'dead chips'.
- A commission on 'live chips'.
- A commission on players' losses.
- A percentage of the casino's theoretical win.

Vulnerabilities

Movement of people and money to casinos

153. A vulnerability of junket programmes is that they involve the movement of large amounts of money across borders and through multiple casinos by third parties. Junket participants generally rely on the junket operators to move their funds to and from the casino. This creates layers of obscurity around the source and ownership of the money and the identities of the players. This is made more difficult if the junket operator is complicit in any money laundering activity by the players, or is solicited by criminals to blend illicit funds with the pool of legitimate funds.

154. Foreign marketing offices/branches of casinos may accept deposits to a patron's casino account before they travel to the casino. The study of casino vulnerabilities could not identify cases where the foreign marketing offices of a casino were subject to local AML/CFT controls, despite their role in taking deposits to player accounts. In such cases there is, in effect, no cross border wire transfer to move the funds to the casino.

Case 24. Criminal control of junket operations

Offence:	money laundering
Jurisdiction:	Australia
Technique:	Use of a junket agent to move funds and purchase chips
Mechanism:	Casino agent

A gambler used gambling contacts and knowledge of high-stakes gambling to become a registered and successful junket operator, bringing millions of dollars of revenue to a casino. All of the money gambled by the junket went through the operator's accounts in order to calculate commission from the group's turnover. This way the casino bypassed the necessity for identifying the source and beneficial owner of the funds. It was not until the junket operator began stealing from her customer's winnings that this situation came to the attention of the authorities.

155. Junket operators may use wire transfers to move funds on behalf of clients. The identity of the junket patrons may be unknown to the sending and receiving financial institution or the receiving casino.

Regulation of Junkets

156. Relatively few casino jurisdictions regulate junkets. While the US has a long history of regulating junkets, as an example Macao, China has only recently taken steps towards clear regulation of junkets and their representatives.

157. In the US, a number of states require registration of junket representatives. As an example, the State Gaming Control Board of Nevada requires a fingerprint check and detailed information including military record and criminal arrests. Macao, China requires licensing and registration as well as fit and proper tests of junket operators, as does Australia. Very few gaming jurisdictions have controls on whether or not junket operators are permitted to extend credit to the players taking part in the junket.

158. In cases where junket operators are strongly regulated, jurisdictions require junket operators to be vetted, licensed and operate according to regulations; some with specific AML/CFT controls that compel junket operators to report suspicious transactions by its players. In addition some legal frameworks place the responsibility for junket activities on the casino operator, with their license at risk if players' funds are found to be unlawful. Strong regimes oblige the casino operators to report any suspicion that a junket promoter may be involved in illegal activity.

159. Some casinos and junket providers operate in a number of jurisdictions and offer services from the same casino group in a number of jurisdictions. It is not clear what obligations are placed on junket operators or casinos when they operate in a number of jurisdictions. In relation to junkets offered by independent operators and by casinos, there are a number of issues with foreign branches or subsidiaries of casinos operating in another jurisdiction to the one where the casino is located.

160. Such issues vary from jurisdiction to jurisdiction, but include the following:

- Over-reliance on junket operators, especially in markets with resident populations that are too small to normally support casinos can pose a heightened money laundering risk. In these instances, casinos can become overly dependent on junket operators for business, a potential misuse of these services.
- In some jurisdictions, a casino may enter into a contractual agreement with a junket operator to rent a private room within a casino and in some situations, it is the junket operator, not the casino, which monitors player activity and issues and collects credit.

- Junket operators that provide premium players may exert commercial pressures on casinos, which may result in reducing scrutiny of individual spending patterns, or unduly influence or exercise control over licensed casino operations.
- Junket operators may engage in lending or the facilitation of lending to players outside casinos' knowledge.
- In some jurisdictions, junket operators are allowed to 'pool' and therefore obscure the spending of individual customers, thus preventing casinos from making any assessment of customers' spending patterns.
- In certain jurisdictions, licensed junket operators act as fronts for junket operators in another country. The front operators supply players to a casino through a casino's licensed junket companies which may not qualify for licensure in the country where the players will be gambling. Such unlicensed sub-junket operators can act as unlicensed collectors of credit and may have ties to organized crime networks.

161. All the above issues pose serious risks, and can lead a casino to engage in informal arrangements with junket operators that are inconsistent with risk-based AML/CFT policies, procedures and internal controls as well as hinder authorities' ability to recognize the level of risk that certain operators pose.

Junkets use of alternative remittance

162. In some jurisdictions junket operators may use formal or informal systems to remit money. The nature of junket business assists them to facilitate informal alternative remittance. The Junket operators may have agents in a number of jurisdictions. Junkets / casino agents may utilise their branch offices in foreign jurisdictions to organise movement of funds to the casino jurisdiction. It is not clear if these agents are responsible to their home jurisdiction for reporting STRs on junket patrons.

Case 25. Cash smuggling and underground remittance

Offence:	Cash smuggling, money laundering
Jurisdiction:	Macao, China
Technique:	Use of an casino agent to move funds and purchase chips, structuring
Mechanism:	Casino, casino agent, remittance arrangements
Instrument:	Cash, cashier's order

A casino agent received large amounts of cash in PR China from a mainland customer who wanted to gamble at a Macao, China casino. The agent took the cash to a shop at Zhuhai, which is adjacent to Macao, China. The shop divided the sum into small lots, which would be carried to Macao, China by many 'professional commuters'. Another agent collected these lots and handed them to the casino agent by depositing the monies into his account in the form of cash, cheque, bank transfer and remittance. When the full sum was received, the casino agent converted it into a cashier's order for receipt by the VIP room of the casino. The VIP room then issued non-negotiable chips to the mainland customer who could start gambling. When the customer won from the table, the gain in cash is given to the casino agent who would remit the funds back to China via underground banks.

Case 26. Use of junket promoter and casino VIP room to move cash between countries

Offence:	Money laundering
Jurisdiction:	Macao, China
Technique:	Use of third parties to move illicit funds
Mechanism:	Casino, junket operators
Instrument:	Cash

A merchant in country A could not perform a large remittance to country B due to its foreign exchange control. With the help of a junket promoter, he transferred the monies to the VIP room of a local casino, which informed

an underground remitter in country B about the amount and beneficiary of the funds. The remitter would then arrange payment of the fund to the beneficiary. For country B citizens who wished to gamble in this casino of country A, but had difficulty in bringing in the cash, they would arrange alternative remittance through this remitter who would then inform details of these customers to the VIP room. When these citizens arrived at the VIP room they could immediately obtain the amount required for gambling. Both the VIP room and the remitter would perform reconciliation for net settlement, and basically no transfer of monies between two sides was required.

Case 27. Junket promoter use of underground banking

Jurisdiction: South Korea
 Technique: Alternative remittance
 Mechanism: trade-based settlement mechanism

A casino in Las Vegas, 'A' operated a marketing team entirely responsible for Korean customers. This team lent gambling money to Koreans in form of card (coupon) not cash so that the loan would be spent only for the purpose of gambling at 'A'. The members of this team visited Korea to collect debts or made their relatives in Korea do so on behalf of them.

The collected money was paid to trading companies in Korea for the goods that these companies sold to importing companies in the United States. And the importing companies paid the amount to 'A'.

Junket incentives – 'Dead chips'

163. Casinos in some regions offer junket agents a commission on non-negotiable, or "dead", chips. The use of dead chips requires the junket operator to account for their use. These 'dead chips' cannot be redeemed for cash from the casino, but are only negotiable with the junket promoter. In general, dead chips can be wagered only in the game of baccarat.

164. Players purchase large amounts of these chips from the junket operator at a discounted price based on an operator's terms. They cannot redeem the chips for cash or for live chips but must play the chips until they lose them or win replacement live chips. The live chips can be redeemed for cash with the casino. At the conclusion of gambling, 'dead chips' can be redeemed with the junket operator. A junket operator requires players periodically to roll their "live chips" into "non-negotiable" dead chips so that an operator can receive a commission from a casino based on the total value of the dead chips. Because 'dead chips' are offered at a premium to junket patrons, there is an incentive for players to purchase additional 'dead' chips and players receive live chips in exchange as well rebates equal to the product of the agreed-upon rebate percentage and total dead chips purchased.

165. ***'Dead chips' being used by criminals as currency*** – jurisdictions report 'dead chips' being used in drug deals and to settle other criminal transactions.

166. ***'Dead chips' being smuggled out of a jurisdiction*** – such chips are a safe way for criminals to move value as they are difficult for customs agencies to detect in cross border movements.

Case 28. 'Dead chips' associated with loan sharks

Offence: money laundering, criminal coercion
 Jurisdiction: Hong Kong; China; Macao, China
 Technique: Use of 'dead chips'
 Mechanism: Junket 'dead' chips

Dealing in junket chips (colloquially known as 'mud-chips') is closely connected to other forms of criminality, and it is particularly ripe for exploitation by loan sharks often with a triad element, who are attracted by lucrative profits and the ease of finding potential borrowers amongst gamblers, with loans being offered in the form of 'mud-chips'.

In Hong Kong, China for example, stooge or nominee corporate accounts are often used for settlement purposes

by loan shark syndicates operating offshore. A common scenario involves victims being induced to gamble more than they can afford in the VIP rooms at offshore casinos by mud-chip (*dead chip*) syndicates, which often work with loan sharks. The victims are then escorted back to Hong Kong, China and held pending settlement. Family members are induced to make settlement by bank transfers, which are structured through a series of stooge accounts.

Case 29. Diversion of illicit funds to casino agents and junket operators

Offence:	Fraud, money laundering
Jurisdiction:	Hong Kong, China, China, United States
Technique:	Use of third parties to move illicit funds
Mechanism:	Casino agents, junket operators
Instrument:	Cash

In 2006, three provincial managers of a bank in another jurisdiction were indicted for embezzling in excess of USD 3.5 billion that was subsequently channelled through shell companies and personal and investment accounts in Hong Kong, China with the help of associates and intermediaries. Approximately HKD500 million was deposited with the representative agents and junket promoters of various South East Asian and North American casinos for the groups' personal use.

167. Indicators of money laundering through junket operations include:

- Players refusing to provide identification.
- Use of representatives/third parties to conduct cash buy-in.
- Junket chips redeemed without any gambling activity.
- Source of funds for buy-in not disclosed.
- Source of funds for buy-in from companies.
- Buy-in of junket chips by a person whose occupation is not commensurate with the buy-in value.
- Junket issuing cheques to rival casinos.
- Junket transferring funds to players with no verifiable proof of winnings.
- Player frequently requesting cheques from junket operator below threshold amounts.

Emerging Issue – Cruise Ship junkets

168. A growing number of independent casino junket representatives now offer junkets to cruise ships. These escorted cruise casino junkets tend to be on ships of the same lines and the packages offered by independent operators range from cruises that are entirely complimentary (with the exception of port charges and taxes) to packages offering reduced player rates. In most cases, players deposit a significant amount of money up front with the independent junket operator. Once aboard, the player can then draw this money for gambling in the cruise ship casino. Very few jurisdictions regulate junket operations linked to cruise ship gaming.

VIP Rooms and ‘High-Roller’ Customers

169. VIP customers or ‘high rollers’ are highly valued casino customers who gamble in private and exclusive rooms within the casino complex and are afforded special treatment by the casino. VIP rooms are closely tied to the junket business, and, like junkets, the vulnerability is with identifying the high rollers, and being able to know where their money is coming from and going to. A concern shared by many jurisdictions is that casino staff view very high cash use or large deposits and withdrawals by VIPs, and especially within VIP rooms, as ‘normal’. In addition casinos offer VIP customers financial facilities akin to any banking institution, yet many jurisdictions do not have the level of AML controls over casinos as they do their banking industry. If there are no requirements to conduct CDD on VIPs, particularly those associated to junkets, and/or regulators and law enforcement cannot access membership information on operations and if required the money trail associated with their gambling, it poses a serious risk.

170. VIP customers represent high revenue streams for most casinos. A Canadian study in 2007 showed VIP customers are responsible for 80% of casino turnover in Canada, but only represented 1% of casino patrons. Macao, China also reports 50-70% of all casino revenue comes from VIP rooms.

171. In the past, under Macao, China’s old monopoly system the VIP rooms catered to clients seeking anonymity and were shielded from official scrutiny. With the changes to the gaming industry in 2002 and passing of new AML/CFT laws in 2006, the casino industry has been placed under the AML/CFT regime with casinos (including gaming intermediaries and junket operators) having obligations to report STRs to the FIU in the main areas and VIP rooms – and with respect to all customers. Macao, China reports that supervisors and casinos are aware of the risk that VIP rooms could be associated with crimes, and have been tightening the control of junket activities. At the same time, all casinos do not cede control of their VIP gaming facilities to outside organisations, which impedes organised crime’s ability to operate in the casino sector.

172. The following two cases illustrate the risks presented by VIP players:

- In Australia a high profile Asian organised crime figure became a member of the high rollers club at an Australian casino. The person was running a heroin trafficking network from suites in the casino’s hotel and using his gambling activities to mask the illicit profits. He was a VIP player with an extremely high turnover. Over a two-year period he was given gambling incentives by the casino of more than AUD 2.5 million dollars and spent two years as a non-paying guest of the casino’s hotel. It was not until he was investigated by law enforcement agency that the casino looked more closely at his gambling transactions.
- In the United States a foreign national travelled frequently to Las Vegas to gamble. He was well-known to a Las Vegas casino and had a gambling loss of approximately USD 1 million over a four year period. Over a subsequent three year period his losses increased to more than USD 125 million. On his behalf the casino conducted wire transfers and direct bank to bank transfers from corporate accounts. The casino on occasion would extend him USD 10 million line of credit and frequently offered him extravagant perks including use of hotel suites, cars, and the casino jet. There were no SARs filed by the casino and no verification of his source of funds was undertaken. Yet open source documents show the company owned by the person could not have generated income sufficient to sustain his gambling losses.

Corrupt or Inadequately Trained Staff

173. Effective AML/CFT controls require casinos (and support industries) to be free from corruption and influence and casino employees to be adequately trained to prevent and detect money laundering activity. However, high staff turnover is characteristic of many casino sectors, particularly in the regions that are poorly regulated for AML/CFT, AML training and experience being lost from the sector as a result. And the potential for corruption in a cash intensive industry, characterised by high employee turnover, is ever-present. Reported cases demonstrate that casino employees, either individually or acting in concert with others, intentionally do not file suspicious/threshold reports, destroy records and falsify documents to disguise money laundering activities. However, inadequate systems and poor employee training also account for large-scale money laundering in the casino sectors.

- In 2007 a number of casino employees were charged for their role in running an illegal gambling ring out of a casino, taking in USD 22 million in sports betting. The casino employees included poker room supervisors, dealers, and a bartender and their roles mostly involved not filing suspicious reports on transactions.
- A Las Vegas compliance officer was charged with failure to file approximately 15 000 CTRCs between 2001 and 2003. He stated that he did not file the reports because he was having personal problems, was behind in his work, and the importance of filing CTRCs was never explained to him.
- In 2006 a drug dealer admitted to distributing approximately 100 pounds of crystal methamphetamine between Las Vegas and Hawaii. In court, he admitted to gambling millions of dollars in cash through Las Vegas Casinos, mostly carried in to the casino in duffle bags. Law enforcement authorities were never notified of this activity.
- USD 207 million in cash was found in a home in Mexico. It is believed to be the proceeds of a drug kingpin who reportedly lost between USD80 – 120 million at Las Vegas Casinos. However, law enforcement authorities were unaware of this person until the cash seizure.

174. Most well-regulated jurisdictions require casino operators to certify an employee's competence to perform the functions authorised by their employment license. This can include reporting of suspicious and significant transactions to the FIU and reporting of illegal and undesirable activity by patrons. Some jurisdictions require regulators to approve the content of training courses run by the casino operator. Yet inadequate employee training, as demonstrated by the cases above, is a significant vulnerability within the casino sector, regardless it seems of the level of regulation imposed.

New Casino Markets

175. As discussed in Chapter 1, new and emerging casino markets are vulnerable to money laundering activities, particularly in the Asia/Pacific and African regions where casino sectors are being rapidly established in developing countries. Many of these jurisdictions have predominantly cash-based economies, poor governance and weak or limited AML/CFT capability. Often the growth of the casino industry will outpace the country's ability to put in place sufficient AML controls, as well as regulatory and enforcement capacity, leaving the sector vulnerable to corruption and money laundering by organised crime groups.

176. Macao, China is another area of vulnerability due to rapid market growth. Revenues in Macao, China started to surge in 2004 when new casinos opened after the 2002 decision to end the 40 year monopoly by the STDM. Now the majority of Macao, China's economy is linked to the casino industry. In less than 6 years, Macao, China has become the biggest casino market in the world. Prior to regulatory reforms in 2002, Macao, China's casino industry was under-regulated, despite the presence of high cash transactions and lucrative junket and VIP room contracts. Since 2002, Macao, China has sought to reform its legal regulatory framework for AML/CFT in the casino sector, however, like many jurisdictions, effective implementation of FATF standards remains a challenge.

177. Like all jurisdictions, Macao, China continues to face threats from organised crime. Whilst AML/CFT implementation in the casino sector is occurring, the scale and speed of growth experienced in the market may result in even greater vulnerabilities for ML.

178. The United States has noted that the rapid growth of new casino markets can provide money laundering opportunities. A US threat assessment in 2005 considered the most notable development in this field is the striking growth of Native American casinos, which have enjoyed double-digit revenue growth for the last ten years, collectively taking in USD 25.7 billion in revenue in 2006, more than twice the amount generated by Nevada casinos.²¹

179. A challenge to establishing effective AML/CFT controls for tribal casinos is coordinating the various regulatory bodies. Tribal gaming is regulated on three levels:

- a) Indian Nations (Tribal Government – Gaming Regulatory Commissions).
- b) State Gaming Agencies.
- c) The National Indian Gaming Commission and federal government agencies, including the U.S. Justice Department, the U.S. Treasury Department and the Department of the Interior.

180. The growth of the Indian gaming market, coupled with overlapping regulatory jurisdictions and limited enforcement resources, has generated concern over the potential for large-scale criminal activity in the Indian gaming industry.

High Seas Gambling

181. High seas gambling (also called boat gambling or floating casinos) involves gaming vessels that travel to international waters to conduct gaming/casino activities. These may be long-distance cruises that have gaming/casinos as side entertainment, or short distance trips that are directed solely at gaming.

182. The phenomenon of gambling in international waters is an issue for all countries with cruise ships registered or operating within their jurisdiction. While many countries prohibit casinos on ships from operating in territorial waters, cruise ship gambling in international waters is not well regulated.

183. Few jurisdictions have regulatory oversight over cruise ship casinos registered to their jurisdiction and fewer have AML/CFT controls over cruise ship casinos. Since cruise ship casinos, with only minor exceptions, are allowed to operate only when in international waters the casinos are largely unregulated. Some steps have been taken within the cruise line sector to self regulate (see

²¹ Associated Press., "Tribal casino revenue up 5 percent nationwide", June 19 2008, http://blog.mlive.com/kzgazette/2008/06/tribal_casino_revenue_up_5_per.html

guidelines published in 1999 by the International Council of Cruise Lines (ICCL).²² It is unknown what general record-keeping or due diligence processes, if any, are carried out by cruise lines or if they report suspicious activities to appropriate authorities.

184. Little is known about the level of risk presented by gambling that is undertaken in international waters. For example, it is unknown what methods are used to transfer funds to and from the cruise ship and any associated money laundering risks.

185. Regulatory control over ‘High seas gambling’ raises complex questions of international law. If AML/CFT laws were to apply, which jurisdictions would have oversight; the jurisdiction from which the ship is operating from, or the jurisdiction where the vessel is registered?

186. Some jurisdictions impose tax and AML regulations on cruise ship lines, such as the United States. Ships registered in the US are subject to income tax and money laundering legislations, meaning that US citizens and permanent residents must declare any income from cruise-ship gambling with Customs on returning to the US and through yearly tax returns. The cruise line is also required to file tax notices for jackpots of over USD 1200. However, there is some question as to whether all US registered ships comply with these requirements, and it is unknown the nature or level of oversight by US authorities.

187. High seas gambling is an issue for many jurisdictions, for example Hong Kong, China, where a number of cruise ships or large luxury vessels, operate from their harbours, with the sole or primary purpose of providing casino gaming in international waters. These vessels sail under foreign flags, so port jurisdictions have difficulty in imposing AML/CFT controls on these “foreign” vessels due to the limitation of extra-territorial jurisdiction.

Case 30. High Seas casinos used to launder proceeds of fraud

Offence:	Money laundering
Jurisdiction:	Hong Kong, China; Australia
Mechanism:	High-seas casino; bank accounts,
Instrument:	Casino

In 2005 five Australian citizens defrauded a superannuation scheme of AUD 150 million. Two of the five men flew to Hong Kong, China and boarded a cruise ship, drawing on the illicit funds while gambling at the ship's casino. After losing approximately AUD 3 million, they cashed in their casino chips and had the remaining funds sent to their personal accounts in Hong Kong, China.

188. The case above highlights how ‘high seas gambling’ poses a money laundering risk to port jurisdictions. The lack of supervision of casinos operating in international waters leaves port jurisdictions exposed to casino-related money laundering risks.

189. It should be noted that the FATF and a number of FSRBs, including the APG, consider AML/CFT controls on cruise ship casinos in the context of a country's ME evaluation if this activity presents a risk of money laundering.

190. Jurisdictions have raised the challenges faced by the issue of extra-territorial jurisdiction over gambling activities beyond flag-flying vessels, as per the current status of international law. There appears to be a need for further consideration of the issue and possible multilateral solutions.

²² Further information can be found at <http://www.cruising.org/industry/tech-intro.cfm>

Terrorist Financing

191. Throughout this report, the term money laundering has also referred to terrorist financing. It should be pointed out that the research undertaken failed to find any reported cases of terrorist financing in the casino sector. This may be due to the characteristics of terrorist financing that make it difficult to detect, characteristics such as the relatively low value of transactions involved in terrorist financing, or the fact that funds can be derived from legitimate as well as illicit sources.

192. It would be a mistake, however, to assume that terrorist financing has not and could not occur in the casino sector. Where funds are derived from criminal activity, then traditional monitoring mechanisms that are used to identify money laundering may also be appropriate for terrorist financing and includes the methods and indicators described in Chapter 2, though these indicators would only support suspicious activity, and may not be identified as or connected to terrorist financing once further investigation is undertaken.

193. It should be noted that transactions associated with the financing of terrorism may be conducted in very small amounts, which may not be the type of transactions that are reflected in the indicators for money laundering. Where funds are from legal sources, it is even more difficult to determine if they could be used for terrorist purposes. Therefore, while terrorist funds may be derived from criminal activity as well as from legitimate sources, transactions related to terrorist financing may not exhibit the same traits as conventional money laundering.

194. The ability of casinos to detect and identify potential terrorist financing transactions without guidance on terrorist financing typologies or unless acting on specific intelligence provided by the authorities is significantly more challenging than is the case for potential money laundering and other suspicious activity.

195. Detection efforts, absent specific national guidance and typologies, are likely to be based on monitoring that focuses on transactions with countries or geographic areas where terrorists are known to operate or on the other limited typologies available (many of which are indicative of the same techniques as are used for money laundering). Particular individuals, organisations or countries may be the subject of terrorist financing sanctions, in a particular country. In such cases a listing of individuals, organisations or countries to which sanctions apply and the obligations on casinos to comply with those sanctions are decided by individual countries.

CHAPTER 4 - POLICY IMPLICATIONS

196. A number of issues and policy implications have been identified by the APG/FATF casinos project. Many of these relate to implementation issues with the current FATF standards.

Online gaming / online casinos

197. While this study has not included online gaming / online casinos in its scope of enquiry, it is clear that there are a number of related risks and vulnerabilities from online casinos. A number of jurisdictions license physical casinos and online casinos under a similar process. This report notes a significant gap with understanding regional money laundering risks and vulnerabilities from online casinos and online gaming. There is a need for further study in this area and for sharing case studies and regulatory models.

Lack of AML/CFT coverage for casino sectors

198. A number of jurisdictions clearly lack awareness of money laundering and terrorist financing risks in the casino and gaming sectors.

199. A significant number of jurisdictions have limited regulatory controls, including ‘fit and proper’ tests for casino owners, managers and staff, internal controls, etc. A greater number of casinos sectors are not yet subject to any AML/CFT controls, in particular in developing countries. Very few jurisdictions regulate junket operators.

200. ***Vetting, licensing and training relevant employees*** – jurisdictions raised the need to ensure that staff with a potential to impact on the integrity of the casino operation should be vetted and appropriately trained in AML/CFT. There are significant gaps in coverage of staff in some gaming jurisdictions.

201. ***Internal controls*** – Most jurisdictions require casinos to have a documented set of internal controls over almost all aspects of casino operations. Some require the regulator to approve these whilst others require the documented controls to meet a set of specified standards.

Lack of regulatory tools

202. Law enforcement agencies and regulators report the need for and implementation of suitable tools that carry effective, proportionate and dissuasive sanctions to use in the regulation of casinos, which are wilfully negligent in AML. Results of Mutual Evaluations indicate a lack of effective regulatory tools for casinos across members of the FATF and FSRBs.

203. There is a need for further guidance and sharing of best practice models for AML/CFT regulation, supervision and monitoring of the casino and gaming sectors.

Implementation of CDD measures

204. Many jurisdictions have struggled to implement CDD measures in casinos in keeping with the international standards. A number of jurisdictions have not followed the thresholds outlined in the FATF standards (for example opting for a USD 10 000 threshold for CDD).

205. A number of jurisdictions are relying on customers being issued with a casino membership cards for which CDD information is collected at the start of the relationship. Customers are then only required to present the card to identify themselves when transacting over the threshold of USD/EUR 3 000.

206. A number of jurisdictions have noted challenges with determining a suitable timeframe for determining whether transactions are linked for the purposes of determining whether the USD 3 000 is met. Cases have illustrated criminals' awareness of change of shifts with casino staff to seek to avoid reporting requirements.

207. A key issue is that in general casinos are not doing enough to establish source of funds and failing to recognise suspicious activity by their customers. Casino security and marketing systems tend to pay particular attention to customer's financial transactions and gambling behaviours, but mostly in terms of patterns of winning and opportunities to encourage greater participation. There is a need for greater vigilance of patterns of transactions and play, unusual transactions and possible indicators of suspicious transactions.

208. There is a need for jurisdictions to share more case examples of money laundering cases and experience of ways in which effective AML/CFT preventative measures have contributed to detecting and prosecuting cases of money laundering.

Application of AML/CFT controls to casino foreign branches, offices or subsidiaries

209. A number of casino operations are owned or controlled in a jurisdiction other than the one in which the casino is established. It is not clear what AML/CFT obligations are placed on junket when they operate in another jurisdiction. There is an issue in a number of jurisdictions of equivalent AML/CFT controls not being implemented by branch or subsidiary casinos. There is a need for further international guidance and best practice experience with regulating branches and subsidiaries.

Application of AML/CFT controls to casino foreign holding accounts

210. It is not clear what AML/CFT controls are in place over accounts operated in a jurisdiction foreign to the location of the casino. Large casinos may operate marketing offices in jurisdictions other than where the casino is located. Patrons are able to pay in funds to their casino account to be played when they travel to the casino without sending a cross-border wire transfer.

Control of junket operators and their agents

211. A number of jurisdictions that allow junket play do not require registration/licensing and regulation of junket organisers and their agents. The vulnerabilities identified in the previous section raises concerns about the need to ensure that junkets and their agents are not under criminal control/influence and to ensure that financial transactions are transparent and subject to relevant AML/CFT measures.

212. The international standards do not clearly address junket operations, but their role as intermediaries or third parties is a significant concern in many jurisdictions.

213. ***Issues with foreign branches or subsidiaries of junkets*** – as outlined above, a number of junket providers operating in a number of jurisdictions and offer services from the same casino group in a number of jurisdictions. It is not clear what obligations are placed on junket operators when they operate in another jurisdiction.

Regulatory controls over VIP rooms and related facilities

214. There are significant issues with implementation of CDD controls over VIP rooms. In some jurisdictions there are not clear powers for the regulator, FIU or law enforcement to have access and to share information regarding members of casino VIP programs.

215. In some cases VIP gaming rooms are leased to junket operators, who provide the gaming equipment, staff and funds to play in the room. This may be done outside of the CDD and other internal controls of the casino.

216. VIP rooms may offer safety deposit boxes and other facilities that are not subject to AML/CFT controls, but which might represent a vulnerability for AML/CFT.

Regulatory coverage of ‘foreigners only’ casino models

217. As indicated above, a number of jurisdictions have sought to establish casino sectors, but to ban nationals from entering or playing in the casino. This is viewed as a risk management and harm reduction strategy. In some cases this leads to weakened oversight by authorities as there is a perception that risks from money laundering are less under this model. In some cases of very weak supervision, only basic licensing criteria and foreign exchange obligations are enforced on such casinos.

Regulatory control over high-seas gaming

218. As outlined in the previous section, there is a large-scale high seas or cruise ship casino and gaming market, but few jurisdictions regulate or impose AML/CFT controls over the sector. There are significant issues of legal jurisdiction. In very few cases do the ‘flag’ jurisdictions of cruise ships offering gaming services extend their regulation to gaming conducted aboard the vessels in international waters.

Controls over significant contractors, systems and equipment

219. Jurisdictions raised concerns about contractors that supply goods with a potential to impact on the integrity of the casino operation (*e.g.* gaming equipment and computer systems) should be required to be subject to probity assessment.

Lack of AML/CFT capacity / experience by casino regulators

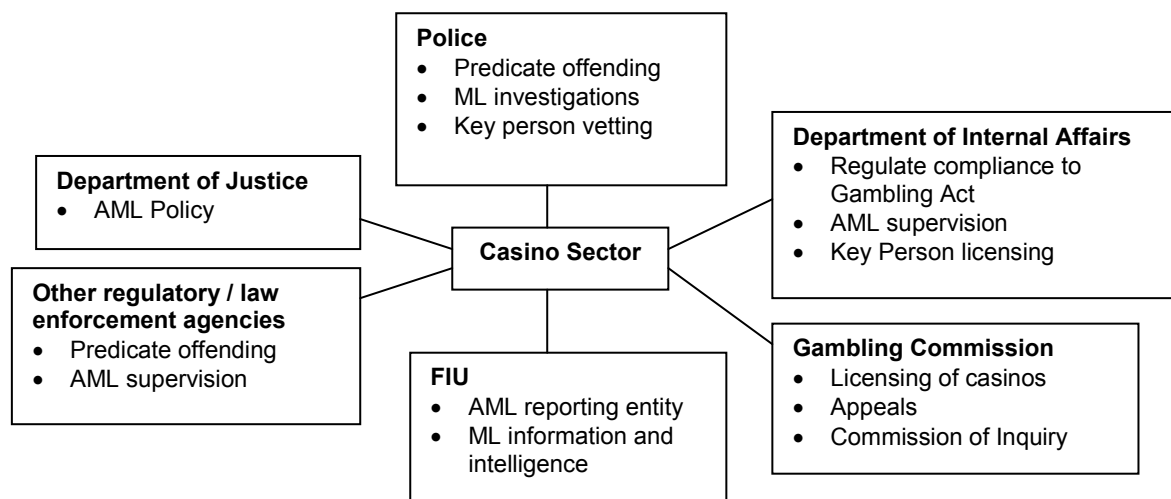
220. In some jurisdictions where casinos have recently been brought under AML/CFT controls, the AML supervisor lacks technical expertise of the casino sector to effectively supervise. There are a number of technical issues specific to casinos and gaming that require sector-specific technical knowledge and experience to support effective regulation and supervision.

Coordination between AML/CFT and casino-sector supervisors

221. Many jurisdictions lack effective coordination between AML/CFT authorities and casino regulatory authorities for setting policies, implementing preventative measures and investigating ML and TF in the sector.

222. In some jurisdictions, a gambling supervisor audits gambling operations in casinos for compliance to gambling laws, but may have a limited role in assessing the casino's level of AML compliance, despite their day to day role. Given the number of financial and non-financial sectors to be supervised, as well as other agencies involved, AML supervision of casinos without the direct involvement of casino regulators may present problems. Joint supervision depends on a high level of inter-agency collaboration to be effective.

223. As shown in the diagram below, New Zealand is an example of a jurisdiction in AML-related policy and operations are invested across a number of agencies.



224. A number of federal systems report state/provincial-level casino regulation, but national level AML/CFT regulation. Effective inter-agency coordination and cooperation is needed to achieve consistent national coverage of casino and gaming sectors for AML/CFT.

Building compliance culture in casino sectors

225. Precluding criminal involvement in casinos and gambling involves addressing both criminal influence and criminal exploitation. Successfully minimising criminal influence of casino operations is dependent upon a licensing and regulatory regime to preclude criminal involvement in the management and operation of casinos and effective preventative measures to detect ML and TF. A number of jurisdictions have struggled to establish an appropriate casino management compliance culture, including for AML/CFT.

226. Persons with large amounts of disposable cash are attractive customers casinos and this makes it imperative that the operator has not only integrity but a commitment to preserving a crime-free environment. Importantly commercial reward systems often provide bonuses or remuneration for “middle management” based on revenue-based performance criteria. These may not take into account the protection of the primary asset (the casino licence) and unless an appropriate management culture is in place within the operator these may work against maintaining a crime-free environment.

227. There is a need for greater cooperation between AML/CFT regulators and enforcement agencies and the front line compliance staff within casinos who are responsible for AML/CFT regulation within casinos.

Law enforcement / FIU / Regulator access to information and investigation of ML/TF

228. **Legislative system for gathering information for law enforcement:** Many jurisdictions provide a legislated system for the regulator to receive requests for casino information (such as patron records) and then direct the casino operator to supply that information to the regulator. The regulator then provides the information to the law enforcement agency without the casino being made aware of which law enforcement agency requested the information.

229. In some jurisdictions this provision is regularly used to obtain lists of the casinos' major players for a set time period.

230. There is a reported need for regulations to oblige casinos to adopt AML- systems, particularly when current arrangements hinder the detection and investigation of money laundering. As an example, most casinos operate player tracking systems (or player loyalty schemes) that record customer's levels of gambling, and can include data such as, capital introduced, wagering amounts, win and loss totals, and turnover. This type of information is critical to identifying and prosecuting money laundering; however, these systems are not calibrated to provide the calculations necessary for investigations or to the evidential standard required of prosecutions. Some jurisdictions report casinos showing very little interest in supporting AML efforts by addressing this issue.

231. **Dedicated police squads or intelligence units:** – In jurisdictions with large urban casinos it is common for there to be a dedicated police squad (sometimes located on site) or a specific police casino intelligence/investigation unit.

232. An important intelligence function for this type of body is being a gathering point of all available criminal intelligence related to casino operations (including from the casino operator and regulator). It is important that such specialist functions should work closely with AML investigations units.

233. **Police barring of undesirable patrons:** – A number of jurisdictions have provided the head of the Police with the power to require casinos to bar specified patrons where there are grounds to believe the person might attempt to criminally exploit the casino if allowed to attend. This is generally on the basis of criminal history or in some cases intelligence information. In some jurisdictions this has been made non-appealable and non-reviewable.

234. **Regulator barring of undesirable patrons:** – A number of jurisdictions have provided the casino regulator with the power to bar or require – casinos to bar specified patrons. This is generally a power reserved for patrons who have not given the casino or police adequate reason to bar the person but owing to information available to the regulator, the regulator is of the opinion that the person is an unacceptable risk to the integrity of the operation of the casino. In some jurisdictions this has been made non-appealable and non-reviewable.

235. **Casino regulator assistance to FIU:** – In many jurisdictions the casino regulator proactively assists the flow of AML/CTF information to the FIU by conducting inspection programs or audits which seek to identify suspicious activity which the casino operator or regulator then reports to the FIU and/or law enforcement. There needs to be close cooperation between the FIU and gaming regulators.

International Cooperation

236. Effective international cooperation remains a challenge for AML and casino regulatory authorities on AML issues in many jurisdictions. Jurisdictions responses indicated relatively low levels of international cooperation between casino regulatory authorities on issues relevant to AML. In addition, several Asian jurisdictions report the difference in legal frameworks between jurisdictions as a factor, as well as their inexperience in AML/CTF supervision and international information exchange.

237. Effective mechanisms are not always in place, in particular to share information related to junket operators and patrons of junket businesses. There is a need for both casino jurisdictions and those jurisdictions whose citizens regularly travel to casino jurisdictions to ensure clear channels for information sharing and cooperation. This is a challenge when a number of the large casino sectors, such as that in the US, are characterised by a large number of state/provincial/city based regulators.

238. The issues described above in no way represent all of the problems encountered by jurisdictions.

Conclusion

239. While it is estimated that 100 countries participate in casino and card room gambling,²³ this research was able to confirm 77 jurisdictions with legalised casino sectors and 8 jurisdictions who have recently legalised or are giving consideration to legalising casinos. This represents a significant global activity that is cash intensive, competitive in its growth and vulnerable to criminal exploitation. What is encouraging is that all 77 jurisdictions are members of FATF or other related FSRBs, requiring those jurisdictions to meet an international standard in their AML programmes.

240. Mutual Evaluations have shown that globally, that while low, the casino sector has shown relatively higher levels of compliance with FATF standards than other DNFPBs. This is largely because of historical concerns many government have over the perceived levels of criminality and social consequence inherent in casino operations. Governments also tend to impose more stringent supervision and record keeping on casino operations in order to track and secure government revenues. For these reasons, it is often less politically difficult to apply AML/CFT measures to casino sectors, compared to other DNFPBs. Despite this there are many jurisdictions that are yet to fully extend AML controls to the casino sector, and as demonstrated by this research, not all jurisdictions have effective controls over the casino sectors even if they are included in AML frameworks.

241. There are significant regional and global sector vulnerabilities and emerging issues that have weakened AML controls and provide opportunity for money laundering and other financial crimes to flourish.

242. A key issue is casinos not doing enough to establish source of funds and failing to recognise suspicious activity by their customers. Casinos have to pay particular attention to customer's financial transactions and gambling behaviours, particularly if it does not correspond to that of a normal gambler or the intention to play to win is apparently absent or secondary. The methods and indicators in Chapter 2, the sector vulnerabilities and emerging issues in Chapter 3, and the policy implications in Chapter 4 are written to provide government decision-makers and supervisors with the base material from which they can properly target policies and interventions based on the pervasiveness of these methods and issues in their country. But more importantly the material in these chapters, specifically

²³ Casino City.

the methods, case studies and indicators, can and should be shared with casino operators and their staff who are on the front line in confronting these activities, so they may put effect to the AML controls imposed on their operation.

243. Indicators are not of themselves evidence of money laundering and it is not the casino's responsibility to determine that money laundering activity is taking place, rather it is the casino's role is to identify and report the suspicious activity. It is then up to the FIU and law enforcement authorities to examine the matter further and determine if there is a link to money laundering or terrorist financing.

BIBLIOGRAPHY

- “An Analysis of the Economic Impact of Indian Gaming in 2006”, *National Indian Gaming Association*, http://www.indiangaming.org/info/pr/press-releases-2007/NIGA_econ_impact_2006.pdf. Accessed at 13 July 2008.
- Aninat, E. Hardy, D. & Johnston, Barry R. "Combating Money Laundering and the Financing of Terrorism", *Finance & Development*, Vol. 39, No. 3, September 2002.
- “A guide for cruisers who enjoy casino VIP privileges.” *Cruise-Casinos*, 2004, <http://www.cruise-casinos.com/jackpots.htm>.
- Australian Casino Economic Report 2005/06”, July 2007, *Australian Casino Association*, <http://www.auscasinos.com/documents/publicationsSubmissions/ACAFinalReport200506v3.pdf>
- Casino City, <http://www.casinocity.com/casinos>, Accessed 16 July 2008.
- Corcoran, B. "Betting on (non-) compliance in South Africa", *Money Laundering Bulletin*, Informa UK Ltd.
- Department of Internal Affairs. *Gambling Expenditure Statistics 1983 – 2007*, [http://www.dia.govt.nz/Pubforms.nsf/URL/Expendstats07.pdf/\\$file/Expendstats07.pdf](http://www.dia.govt.nz/Pubforms.nsf/URL/Expendstats07.pdf/$file/Expendstats07.pdf)
- Global Gaming Business., “Asia Update”, June 2008.
- Ernst & Young, *Reviewing the Market: The 2008 Global Gaming Bulletin*, 2008
- Ernst & Young, *Global Gaming Bulletin 25th Anniversary Edition*, 2007
- European Commission - “Study of gambling services in the internal market of the European Union - Final Report” 14 June 2006, Swiss Institute of Comparative Law, www.isdc.ch , accessed September 2008
- French National Institute of Demographic Studies, http://www.ined.fr/fichier/t_telechargement/15700/telechargement_fichier_en_publici_pdf2_pesa436.pdf, Accessed 3 August 2008.
- Geller, R. “Saturation or Malaise?” *Global Gaming Business*, June 2008.
- Global Gaming Business., “Casinos, Mon!”, June 2008.
- Guilano , D. “Meet in the Middle: An Update on Gaming in Central America”, *Global Gaming Business*, June 2008.
- Monaghan, S. "Presentation on Understanding Gaming in the Far East", *13th International Conference on Gambling and Risk Taking*, May 2006.

“Overview of Gaming Worldwide”, *Casino City, Global Gaming Almanac*, 2007, <http://www.casinocitypress.com/GamingAlmanac/globalgamingalmanac>, Accessed 5 July 2008.
PricewaterhouseCoopers., “Economic Crime: People, Culture and Controls”, 2007, <http://www.pwc.com/extweb/home.nsf/docid/29CAE5B1F1D40EE38525736A007123FD>, Accessed 29 July 2008.

Ricardo. C. S. Siu., "Formal Rules, Informal Constraints and Industrial Evolution - The Case of the Junket Operator Regulation and The Transition of Macao's Casino Business", *UNLV Gaming Research and Review Journal*, Vol. 11, Issues 2, 5 February 2007.

ACRONYMS AND ABBREVIATIONS & GLOSSARY

AML/CFT	Anti Money Laundering and Countering the Financing of Terrorism
APG	Asia Pacific Group on Money Laundering
AUSTRAC	Australian Transactions Reports and Analysis Centre
BSA	Bank Secrecy Act (United States)
CFTAF	Caribbean Financial Action Task Force
CDD	Customer Due Diligence
CPV	Chip Purchase Voucher
CTRC	Currency Transaction Report - Casino
DICJ	Gaming Inspection and Coordination Bureau (Macao, China)
DNFPB	Designated Non-Financial Businesses and Professions
ESAAMLG	The Eastern and South African Money Laundering Group
EAG	The Eurasian Group
EU	European Union
FATF	Financial Actions Task Force
FBI	Federal Bureau of Investigations (United States)
FINCEN	The Financial Crimes Enforcement Network (United States)
FHA	Foreign Holding Account
FINTRAC	The Financial Transactions Report Analysis Centre of Canada
FIU	Financial Intelligence Unit
FSRB	FATF-Style Regional Body
GIABA	Intergovernmental Anti Money Laundering Group in Africa
IGRA	Indian Gaming Regulation Act (United States)
IMF	International Monetary Fund
IRS	Internal Revenue Service (United States)
ME	Mutual Evaluation
MONEYVAL	The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Europe)
MENAFATF	Middle East and North African Financial Action Task Force
PACGOR	Philippine Amusement and Gaming Corporation
PEP	Politically Exposed Person
POI	Person of Interest
RCMP	Royal Canadian Mounted Police
SAR	Suspicious Activity Report
STDM	Sociedade de Turismo e Diversões de Macao, China
TITO	Ticket In/Ticket Out
VLT	Video Lottery Terminal
VIP	Very Important Player

GLOSSARY OF COMMON CASINO TERMS

The bank	The casino
Barred / banned	A person who is not permitted to enter a casino (may be banned by the casino itself or the regulator)
Betting Limit	For table games, the minimum and maximum amount of money that a player is allowed to wager in a single bet
Bill changer	A machine which accepts coins or currency notes and exchanges them for currency notes or coins
Blackjack	A casino card game. Players bet against the dealer
The Cage (cashier's cage / casino cage)	A secure area within the casino which has custody of funds and provides banking services to casino patrons
Chips	Casino value instruments. Issued by casinos and used in lieu of cash in gaming transactions between the house and player. Chips are round and marked with the denomination and name of the casino and are negotiable within the casino
Dead chips	Promotional or junket associated casino chips that cannot be exchanged for cash. See <i>Mud Chips</i> and <i>non-negotiable chips</i>
Even money bet	A wager that pays back the same amount that was originally wagered, plus the original wager.
Even money exchange	Exchanging two items of equivalent value in the casino, such as purchasing USD 100 in chips for USD 100 cash
Float	The amount of value (chips + cash) on a table game
High rollers	Premium players who consistently gamble high stakes and large sums of money – see also <i>VIPs</i> and <i>whales</i>
House	The casino
Junket	A group of people who travel to the casino primarily to gamble. The junket may include transport, accommodation, incentives to play at the casino and the transportation of funds to and from the casino
Junket agent	A person or company who signs up casino patrons to take part in junkets
Junket representative	The person who organises the junket
Mud chips	Promotional or junket associated casino chips that cannot be exchanged for cash. See <i>Dead Chips</i> and <i>Non-negotiable chips...</i>
Non-negotiable chips	Promotional or junket associated casino chips that cannot be exchanged for cash. See <i>Dead Chips</i> and <i>Mud Chips</i>
Pit	An area in the casino where gaming tables operate
Pit boss	A casino supervisor responsible for gaming on the casino floor
Plaques	Casino value instruments. Issued by casinos and used in lieu of cash in gaming transactions between the house and player. Rectangular, square-shaped or oval cheque primarily used in European casinos
Slot machines	Gaming machines that accept coins or vouchers and pay out winnings either in coins or via cashier's cheque
Ticket-in-ticket-out	A cashless slot machine that uses vouchers instead of chips or coins
VIP	Premium players who consistently gamble high stakes and large sums of money – see also <i>Highrollers</i> and <i>whales</i>
Wager	A bet of value
Whale	A high-stakes player

APPENDIX 1. REGIONAL DATA ON CASINO SECTORS

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Africa						
Benin	Yes	1		No		
Botswana	Yes	10			None	Only two casinos operate gaming tables with the reminder operating only slot machines. Both the casinos with gaming tables are subsidiaries of South African casinos. A bill to include casinos under AML/CFT regime is being drafted.
Cameroon	Yes	3				
Central African Republic	Yes	2				
Comoros	Yes	3		Unclear		
Cote d'Ivoire	Yes	1		Unknown		Abidjan Hotel Ivoire Inter-Continental & Casino
Democratic Republic of the Congo	Yes	1		No		

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Djibouti	Yes	1		Unknown		
Egypt	Yes	25				
Gambia	Yes					Kololi Casino, African Gaming Co. Ltd. – Royal 7's
Ghana	Yes	3				Run by KaiRo International.
Kenya	Yes	15				Controlled by the Betting Control & Licensing Board, Mombasa
Liberia	Yes	1				
Madagascar	Yes	2		No		
Malawi	Yes	1+		No		
Mali	Yes	1		No		Run by KaiRo International.
Mauritius	Yes	7+		No		
Morocco	Yes	8?		Yes		
Mozambique	Yes	3		No		
Namibia	Yes			No		
Nigeria	Yes	2				
Reunion	Yes	4				
Senegal	Yes	4				

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Seychelles	Yes	3				
Sierra Leone	Yes	1		No		Licensed, but no supervision by government.
South Africa	Yes	45		Yes		**More details**
Swaziland	Yes	3			Yes	licensed online operators
Tanzania	Yes	3				
Tunisia	Yes	3		No		Only open to foreigners.
Uganda	Yes	3				
Zambia	Yes	3				
Zimbabwe	Yes	6			Yes	Lotteries and Gaming Act, 2000 -Ministry of Home Affairs is the regulator. Limited CDD obligations
Middle East						
Israel	Yes	4				NB – two of these casinos are cruise-ship based casinos
Lebanon	Yes	1				
Central Asia						
Kazakhstan	Yes	28				Since April 2007 laws passed to limit casinos to two provincial cities — Kapchagai (near Almaty) and Shchuchinsk.
Kyrgyzstan	Yes	18		Yes	Yes	MER noted that casinos are showing some resistance to AML/CFT implementation.

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Turkmenistan	Yes	2				
Asia/Pacific						
Cambodia	Yes	21		No	No	Cambodian nationals are prohibited from entering casinos
Chinese Taipei	No		Yes			Press reports indicate that in late 2007 the Chinese Taipei legislature was considering a draft gambling bill which, if passed, would legalise casinos and gaming in Chinese Taipei
Hong Kong, China	No				No	Foreign registered vessels operate casinos in international waters.
India	Yes	6		No		Offshore – limited to the state of Goa
Japan	No		Possibly		No	
Korea, South	Yes	17		Yes	No	
Korea, North	Yes	1		No		
Lao PDR						
Macao, China	Yes	31		Yes	No	3 concessionaires and 3 sub-concessionaries operate all the casinos in Macao, China. Annual revenue is over USD 13.8 billion per annum
Malaysia	Yes	1		Yes	No	
Myanmar	Yes	4		No		The established casinos are not clearly legal.
Nepal	Yes	6	No	No	Yes	Nepal nationals are prohibited from entering. No 'fit and proper' tests for licensees

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Palau	No		Yes		No	Proposals for legalising casino sector have not been supported.
Philippines	Yes	14		No	Yes	All 14 casinos are government owned and operated by PAGCOR. PAGCOR operates an internet casino run in conjunction and cooperation with PhilWeb Corp Approximately 20% of patrons are foreign nationals - Chinese Taipei, Japan and Hong Kong, China.
Singapore	No		Yes	Yes	No	
Sri Lanka	Yes	9		No		Nationals are not allowed into Sri Lankan casinos. Casinos are not clearly regulated by the government, although tax is paid. There is no 'fit and proper' test for casino licensees.
Thailand	No		Possibly			Initial risk assessment from illegal gaming sector undertaken
Vietnam	Yes	2		Yes	No	
Australia	Yes	13	No	Yes	Yes	State-based casino regulation, with FIU national AML/CFT regulator.
New Caledonia	3					
New Zealand	Yes	6	No	Yes	No	Regulator is
Northern Mariana Islands	1					
Papua New Guinea			Yes	No	Yes	Newly passed legislation, May 2007
Solomon Islands	2					
Vanuatu	Yes	2	Yes	Yes	No	No 'fit and proper' tests for casino licensees. Vanuatu licensed an online casino, but it no longer in

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
						operation since 2002.
Europe						
Albania	Yes	1				
Austria	Yes	12		Yes		
Belarus	Yes	Approx 25		Yes		
Belgium	Yes	9		Yes		
Bosnia & Herzegovina	Yes	1				
Bulgaria	Yes	7				
Croatia	Yes	15				
Northern Cyprus (Area of)		Approx. 20				
Czech Republic	Yes	158		No		2004 -27 licenses for 158 casinos across the country. 15 licensed for foreign exchange
Denmark	Yes	6		Yes		
Estonia	Yes	75				
Finland	Yes	1 + some in Åland		Yes Unclear if Åland is covered.	Some in Åland.	Casinos also operating on ships.

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
France	Yes	161		Yes		Widespread casino and gaming industry
Georgia	Yes	10		Yes		
Germany	Yes	62				Widespread casino and gaming industry. Casino regulators at state level. AML/CFT is a federal role
Gibraltar	Yes	1			Yes	19 online casino licensees offering 166 sites.
Greece	Yes	9		No		
Hungary	Yes	6		Yes		
Ireland	No				No	A number of private gaming clubs operate casino-like facilities that create an AML/CFT risk, but which fall outside the scope of the CJA (1994).
Italy	Yes	5		Yes		Although legislation has been adopted bringing casinos within the scope of the AML Law, further regulations are required to implement it.
Latvia	Yes	14		Yes	Yes	
Lithuania	Yes	18		Yes		
Luxembourg	Yes	1				
Malta	Yes	3		Yes	Yes	Regulated by the Lotteries and Gaming Authority 266 online gaming sites are operating. Malta regulates junket providers
Moldova	Yes					

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Monaco	Yes	4				
Netherlands	Yes	167		Yes		
Poland	Yes	27		Yes		FIU is the casino regulator for AML/CFT purposes <i>The Ministry of Finance gives licenses, approves rules of the games in casinos, issues certificates of profession and registers gambling devices.</i>
Portugal	Yes			Yes	No	
Romania	Yes	20		Yes		The number of tourists who come especially to gamble in the Romanian casinos is very little, even insignificant (approximately 40-50 persons/month).
Russia	Yes	169		Yes – the FIU	Yes	After 1 July 2009, all gaming will be prohibited in Russia, except within 4 newly created special gaming zones in Kaliningrad, Rostov-na-Donu, Altai and Primorie Krai (Vladivostok).
Serbia & Montenegro	Yes	7				
Slovakia	Yes	4			1	
Slovenia	Yes	23 + 36 gaming saloons		Yes		Office for Gaming Supervision is the regulator. The 23 licenses for Casinos are mainly owned
Spain	Yes	39 + 2 branches		Yes	No	Approx 3.5 million visitors per annum to Spain's casinos. Regulator is the Ministry of Interior through the National Police.

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Sweden	Yes	4	No. Casinos Act allows for a maximum of 6 casinos	AML only	No	Sweden does not permit internet casinos. MER noted Swedish businesses marketing Malta-based internet casinos in Sweden. Swedish National Gaming Board is the regulator - www.lotteriinspektionen.se
Switzerland	Yes	19	No	Yes	No	
Ukraine	Yes	45		Yes		Over 50 000 patrons visit Ukrainian casinos daily. Ministry of Finance is the licensing body.
United Kingdom	Yes	140 operating casinos		Yes	Yes	Regulations have permitted operators to apply for an online casinos license only since 2007. Regulator: The Gambling Commission - http://www.gamblingcommission.gov.uk
The Americas & Caribbean						
Antigua & Barbuda	Yes	6			yes	
Argentina	Yes	80				Regulated at the provincial level
Aruba	Yes	10				
Bahamas	Yes	4		Yes	No	Tourism Board is the general and AML regulator
Barbados	Yes	2				
Belize	Yes	2			Yes	
Canada	Yes	63		Yes	No	<i>Cruise ship casinos.</i> Cruise ships can offer casino facilities under strict conditions in Canadian waters, but are not covered by the AML/CFT legislation.

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Chile	Yes	17				In 2005 a new Casino Law was passed for a maximum of 24 casinos
Colombia	Yes	20				ETESA regulates all gambling
Costa Rica	Yes	35		No	Yes	more than 250 sports betting companies operate as online casinos
Dominican Republic	Yes	32		No		There is no monitoring of the financial behaviour of casinos or supervision of their AML compliance.
Ecuador	Yes	13				
El Salvador	Yes	2				
Guyana	No					
Haiti	Yes	2				
Honduras	Yes	3				
Jamaica	Yes	10		No		
Martinique	Yes	2				
Mexico	Yes	Up to 5		No		Temporary permits for large-scale “salones de Apuestas”. Regulator is the Secretaría de Gobernación (Ministry of Interior)
Netherlands Antilles	Yes	26				
Nicaragua	Yes	10				
Panama	Yes	36		Yes	1 not yet functioning	

Jurisdiction	Casinos operating	Number of Casinos	Proposals for new Casinos	Regulated for AML/CFT	Online casinos	Miscellaneous
Paraguay	Yes	3				
Peru	Yes	7				
Puerto Rico	Yes	18				
Saint Vincent & the Grenadines	Yes	2				
St Kitts and Nevis	Yes	2				
Suriname	Yes	9		No		
Trinidad & Tobago	No			No		No legal casinos but the 72 Private Members Clubs (registered) seem to operate like Casinos, but are not supervised.
USA	Yes	845		Yes	No	Various US gaming jurisdictions regulate junket operators and their agents.
Uruguay	Yes	18				
Venezuela	Yes	5				