

Anti Money Laundering and Countering Finance of Terrorism Policy

Version 1.0

Document Type	Anti Money Laundering and Countering Finance of Terrorism Policy
Document Owner	PlaySmart ENT BV
Review Frequency	Annually, or when there's changes

Document Control

Business Area	Name	Job Title
Compliance	Marija Rnjak	MLRO

Change History

Version	Date	Author	Details
1.0	30 August 2024	Marija Rnjak	Created initial document
	28 January 2025	Marija Rnjak	Revised and updated document

Anti-Money Laundering (AML) Policy Statement

PlaySmart ENT BV is committed to maintaining the highest standards of compliance with Anti-Money Laundering (AML) regulations and best practices, in alignment with our obligations in the online gaming industry. This statement outlines our policy framework to prevent, detect, and address any activity that could be associated with money laundering, terrorism financing, or other financial crimes.

Purpose

The purpose of this AML Policy is to:

- Establish a clear and robust framework to mitigate risks associated with money laundering and related financial crimes.
- Ensure compliance with the laws and regulations mandated by the Curacao gaming regulator and other applicable jurisdictions.
- Safeguard the integrity of the Company, its customers, and the broader financial ecosystem.

Section 1 – Introduction

Purpose of the Policy

This Policy provides guidance on the procedures to be followed to ensure that operator brands on Playsmart gaming platform comply with the various anti-money laundering and counter financing of terrorism requirements placed upon us and to assist you in understanding your personal obligations under the legislation.

Who does the Policy apply to?

This Policy applies to all staff, management, and directors of the Business.

It should be read in conjunction with any guidance issued from time to time by the Money Laundering Reporting Officer (MLRO).

Whilst appropriate training will be provided on an ongoing basis, all staff must ensure that they are fully conversant with the AML/CFT Policy.

The Employee Handbook also contains extracts from this policy as follows:

- Obligations of the company and employees
- Definitions
- Types of Offences
- A list of the relevant legislation and regulations that apply
- Reference to the Money Laundering Reporting Officer and who the person is

If you are unsure as to how to apply any of these procedures or need more guidance, please speak to the MLRO.

Appointment of a Money Laundering Reporting Officer (MLRO)

A specific person is appointed to receive notifications of internal reports of knowledge or suspicion of money laundering or terrorist financing. This person is commonly referred to as the MLRO and the alternate is known as the Nominated Officer.

Responsibilities:

The ultimate responsibility for the AML framework rests with the Board of Directors and the Money Laundering Reporting Officer (MLRO). The MLRO is responsible for AML issues:

- Owning and overseeing implementation of a dynamic risk-based AML Policy
- Receive internal suspicious activity reports, review, and submit externally as required
- Oversee, review and challenge risk assessments produced by the Business
- Provide AML training to employees
- Report to the Board at least annually on AML within the business (the MLRO has
- direct access to the Board which is responsible for managing the company's money
- laundering and terrorist financing risks.)
- Sit on the Compliance Committee and provide updates on AML to the Committee

MLRO Responsibilities include;

Responsibility for updating this Policy

The MLRO is responsible for reviewing the contents of this Policy on an ongoing basis to ensure that procedural and / or regulatory or legislative amendments are reflected in the Policy.

Monitoring compliance with this Policy

Regular monitoring is in place to test the operation of anti-money laundering and counter financing of terrorism procedures and controls. The compliance monitoring programme reviews the firm's compliance with the anti-money laundering procedure.

The business also monitors and tests the effectiveness of the anti money laundering training by testing the employee knowledge of the requirements set out in the AML training programme.

All employees must also sign electronically, on an internal documents system, that they have read and understood the latest AML Policy. This check is monitored by the Compliance Internal Audit function.

Section 2 – Background

What is money laundering?

As a licensed operator, the Business has a responsibility to uphold the three licensing objectives set out in the Gambling Act 2005 (the Act). The first of those licensing objectives is to prevent gambling from being a source of crime or disorder, being associated with crime and disorder, or being used to support crime.

Money laundering in the gambling sector takes two main forms:

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

Defining what is meant by the proceeds of crime and money laundering

Broadly, the term 'proceeds of crime' or 'criminal proceeds' refers to all property from which a person benefits directly or indirectly, by being party to criminal conduct, for example, money from drug dealing or stolen in a burglary or robbery (this is commonly referred to as criminal property). It also includes property that a person gains by spending the proceeds of criminal conduct, for example, if a person uses money earned from drug dealing to buy a car or a house, or spends money gained in a bank robbery to gamble. Typically, classic money laundering consists of a number of stages:

- Placement
- Layering
- Integration

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

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

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

There is potential for money launderers to use gambling at every stage of the process. The land-based gambling industry is vulnerable during the placement stage and operators are therefore required to ask customers about the origins of cash and to report any suspicions. The remote gambling industry is vulnerable through identity fraud which can enable the money launderer to move criminal proceeds with anonymity by hiding behind stolen ID and payment instruments. Furthermore, the use of multiple internet transactions can facilitate the layering stage of money laundering.

Operators should be mindful that the offence of money laundering also includes simple criminal spending (the use of criminal proceeds to fund gambling as a leisure activity) and may not include all the typical stages of the laundering process (if any at all). Regulators have been highly critical and have imposed heavy penalties on operators who have accepted funds later discovered to be the proceeds of crime.

How the Business might be affected by money launderers

The Business is most likely to be used by money launderers at the Layering stage where criminals may use our products and services to assist them in obscuring the trail and the use of the proceeds of crime to fund gambling activity.

What is Terrorist Financing?

It is a criminal offence for someone to provide or collect funds that they know, or suspect are intended for use to fund terrorist groups or acts of terrorism. Terrorist financing works slightly differently to money laundering in that the funds start off "clean" but are used for illegal acts. The process of disguising where the funds are destined is, however, similar to the way in which money launderers disguise the illegal origin of their funds. Funders of terrorism will attempt to obscure or hide the true beneficiary of transactions or a number of transactions involving relatively small individual amounts. As such, the patterns of transactions or behaviour that ordinarily indicate an unusual underlying activity are much more difficult to detect. Proper due diligence in relation to each customer and the purpose and intended nature of the business relationship is therefore essential in the fight against terrorist financing.

The Terrorism Act establishes several offences about engaging in or facilitating terrorism, as well as raising or possessing funds for terrorist purposes. It establishes a list of proscribed organisations that are believed to be involved in terrorism. The Terrorism Act also contains defences to the principal terrorist property offences.

The Terrorism Act applies to all persons and includes obligations to report suspected terrorist financing. The Business will therefore report instances of suspected terrorist

financing to the NCA using the same methods as those for the reporting of known or suspected money laundering activity.

The Legislation/Regulations

The law relating to anti-money laundering and counter financing of terrorism is contained in several different Acts and guidance.

The main Acts and sources of guidance are:

- EU Money Laundering Framework, Regulations & Directives
- Proceeds of Crime Act 2002 (“POCA”)
- Gambling Act 2005
- UKGC Licence Conditions and Codes of Practice
- UK Money Laundering, Terrorist Financing and Transfer of Funds (Information on Payer) Regulations 2017
- UKGC Guidance
 - Duties and responsibilities under the Proceeds of Crime Act 2002 (issued October 2017) and
 - The prevention of money laundering and combating the finance of terrorism Fifth edition, revision 2 (issued 15 February 2021 to clarify high-risk countries applying to UK, replacing EEA)
- HMRC National Risk Assessment of ML and TF December 2020 (informing UKGC 5th edition guidance)
- Alderney Gambling Control Commission - Internal Control System (ICS) Guidelines
- Financial Action Task Force (“FATF”) guidance and recommendations, including March 2021 Guidance on Risk Based Supervision

The Key Offences

All members of staff and management have personal obligations under the legislation to ensure that no assistance is provided to Money Launderers in any way. Anti-Money Laundering and Countering the Financing of Terrorism Policy These offences relate to the concealing, disguising, converting, transferring, acquisition, use and possession of criminal property, as well as an arrangement which facilitates the acquisition, retention, use or control of criminal property. For example, in the gambling industry, this may involve the taking of cash, cheque or card payments, based on funds which are the proceeds of crime, in the form of a bet or wager, or holding money on account for a customer for the purposes of gambling.

These offenses are typically categorized based on various stages of money laundering activities, such as the placement, layering, and integration of illicit funds. Here are some of

the main offenses:

- Concealing or Disguising Criminal Property

Employees must ensure they do not engage in or facilitate any actions aimed at concealing or disguising criminal property, including but not limited to transferring funds into accounts with the intent to hide their true origin.

- Transferring Criminal Property

It is prohibited to facilitate or participate in the transfer of criminal property or the proceeds of crime. This includes transferring funds or assets with the knowledge that they have been derived from illegal activities.

- Acquiring, Using, or Possessing Criminal Property

Employees must avoid acquiring, using, or possessing criminal property. If there is any suspicion that property may be derived from criminal activity, it should be reported immediately.

- Failure to Report Suspicious Activity

Employees are required to report any suspicious transactions or activities immediately to the designated compliance officer or directly to the relevant authorities. Failure to report can result in criminal prosecution.

- Money Laundering (Direct Participation)

Direct participation in money laundering activities, whether in the form of placement, layering, or integration of criminal property, is strictly prohibited and will result in severe penalties, including criminal prosecution.

- Providing Financial Services to Facilitate Money Laundering

Any employee or third party providing financial services with the knowledge or intent to facilitate money laundering or the movement of illicit funds will face legal consequences.

- Tipping Off (Prejudicing an Investigation)

Employees are strictly prohibited from tipping off individuals or entities who are the subject of a suspicious activity report or any related investigation. This offense is punishable by law

- Engaging in Trade-Based Money Laundering

Engaging in or facilitating trade-based money laundering activities, such as misrepresenting the value of goods and services, is a serious violation of AML regulations and will not be tolerated.

- Structuring (Smurfing)

Engaging in structuring, or smurfing, to avoid detection of large transactions is considered a form of money laundering and is prohibited.

- Assisting with the Integration of Criminal Funds

Any activity that assists in the integration of criminal funds into the legitimate economy, including investments, asset purchases, or business operations, is prohibited.

The Financial Action Task Force ("FATF")

The FATF is the collective name for a group of countries who have established a common set of standards aimed at preventing money laundering. A link to the FATF website is available [here](#). The member countries of the FATF are required to adopt these standards. The FATF has also introduced a series of "Special Recommendations on Terrorist Financing" which place certain obligations on its member countries. The Business is committed to complying with any related measures introduced by other relevant bodies.

Sanctions and Notices

In accordance with the requirements of the **Curacao Gaming License** and applicable international anti-money laundering (AML) regulations, our organization maintains a strict policy regarding **sanctions and notices**.

We are committed to ensuring that no transactions, activities, or individuals associated with our operations involve parties subject to financial sanctions or regulatory restrictions. This includes individuals or entities listed on sanction lists issued by relevant authorities such as the **United Nations, European Union, U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC)**, and others.

In the event that a sanction notice is issued, or if a potential or existing customer is identified as being in violation of these sanctions, immediate action will be taken, including freezing accounts, halting transactions, and reporting the issue to relevant authorities in

compliance with Curacao's regulatory requirements. Additionally, our compliance team will regularly monitor and review updates to sanction lists and ensure that all employees are promptly notified of any changes that could impact business operations.

We are committed to transparency, accountability, and adhering to the highest standards of legal compliance in all aspects of our gaming operations.

Zero Tolerance Policy

PlaySmart ENT BV adopts a zero-tolerance policy toward money laundering and financial crime. Non-compliance with this policy will lead to disciplinary action, up to and including termination of employment or customer account closure, and may result in legal proceedings.

Continuous Improvement

We are dedicated to regularly reviewing and updating our AML Policy to adapt to changes in legislation, regulatory requirements, and evolving threats in the online gaming sector.

Conclusion

PlaySmart ENT BV AML Policy reflects our unwavering commitment to ethical practices and compliance. By adhering to this policy, we aim to foster a safe and trusted environment for our customers, regulators, and stakeholders.

Tab 2

