

Proyecto Pro B.V.(PPBV)

Anti-Money Laundering & Counter Terrorist Financing Policy

(Online Channel)

Key Messages

PPBV is required to have established processes in place to prevent and detect money laundering and terrorist financing

The identities of customers must be verified in line with applicable legislation in the relevant jurisdiction

On-going monitoring of customers is performed to ensure that the transactions are consistent with the customer's risk profile within the online estate

Customers assessed as high risk, including PEPs, or any customer that triggers a transaction monitoring threshold is subject to Enhanced Due Diligence

PPBV will submit a Suspicious Activity Report to the appropriate Financial Intelligence Unit where there is knowledge, suspicion, or reasonable grounds for suspicion of money laundering

Statement of Principle

“Through effectively managing the risk of money laundering and terrorist financing, we protect the Betpositivo brand and meet our licensing obligations”.

Introduction

PPBV is committed to high standards of anti-money laundering compliance and requires Directors, Management, Employees, and Contractors to adhere to these standards in preventing the use of its products and services for money laundering purposes. This document, Anti-Money Laundering & Counter Terrorist Financing Policy (Online Channel) sets out the process and controls required to meet this standard and to minimize the risk of the company being abused for the purposes of laundering funds associated with criminal activity or terrorist financing through its online offerings.

Once PPBV holds online operating licenses across multiple jurisdictions, in order to maintain these licenses we are required to have processes in place to prevent and detect money laundering and terrorist financing; and comply with local legislation in each jurisdiction.

The impact of a breach of these obligations to PPBV can be very significant and can include adverse media coverage, reputational damage to the brand, as well as financial or legislative penalties. Therefore, the risks of money laundering and terrorist financing must be effectively managed.

Application

The money laundering in the gambling sector has 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’ spending).

This policy covers both forms of money laundering.

Terrorist financing refers to money or other property which is likely to be used for the purposes of terrorism, proceeds of the commission of acts of terrorism, and proceeds of acts carried out for the purposes of terrorism.

The terrorist financing threat largely involves low levels of funds being raised by individuals to send overseas, fund travel, or fund attack planning. While the risk of terrorist financing through PPBV is low, all staff must be aware of it and report suspicions of terrorist financing immediately. The reporting process is outlined further in this document.

This policy applies to all PPBV online product offerings (including Sportsbook and Gaming), associated functions and all employees. A separate policy document (PPBV Anti-Money Laundering & Counter Terrorist Financing Policy (Retail)) applies to Retail betting shops.

Minimum Standards

This policy provides guidance to employees in relation to the following AML processes:

- Business Risk Assessment (Macro)
- Customer Due Diligence (CDD)
- Monitoring of Customers and Transactions
- PEPs and Sanctions
- Enhanced Due Diligence (EDD)
- Source of Funds and Source of Wealth
- Reporting Suspicious Activity
- Record-Keeping Requirements
- Training & Awareness

Business Risk Assessment (Macro)

As part of our license obligations, PPBV conducts an AML business risk assessment on at least an annual basis which includes both the retail and online estates to identify and evaluate money laundering risks across the business.

The Business Risk Assessment reviews the overall risk profile across the following risk factors:

- Customer risk;
- Product risk;
- Payment risk;
- Location / Geographic risk.

To ensure we have adopted a risk-based approach, several steps are required to assess the most proportionate way to manage and mitigate the risk faced:

- Identifying the money laundering risks relevant to PPBV;
- Designing and implementing policies, procedures, and controls to manage and mitigate the identified risks;
- Monitoring and improving the effective operation of these controls;
- Recording what has been done, and why.

Customer Due Diligence (CDD)

If you “Know Your Customer” (KYC) it is easier to identify suspicious transactions and activity. CDD comprises

- a) identifying and verifying the customer’s identity based on documents or information obtained from a reliable and independent source;
- b) if applicable identifying any beneficial owner and taking reasonable measures to verify that person's identity, and taking reasonable measures to understand the ownership and control structure of the customer;
- c) assessing and, as appropriate, obtaining information on the purpose and intended nature of the business relationship;
- d) conducting ongoing monitoring of the business relationship.

The identities of customers conducting business with PPBV through its online channel must be verified in line with applicable legislation in the relevant jurisdiction. See Appendix A for further details on the CDD requirements in each jurisdiction.

- For a personal customer, CDD consists of (i) obtaining the customer’s Name, Date of Birth, and Address; and (ii) verifying the customer’s Name, Date of Birth, and Address against independent reliable sources such as electronic KYC providers and/or government-issued identity documents.
- For a non-personal entity (a business), CDD usually consists of 3 elements:

-
- i) Evidence of the existence of the Company (usually a Certificate of Incorporation or similar);
 - ii) Evidence of who the Directors are and evidence of the identity of 2 Directors;
 - iii) Evidence of the ownership structure and evidence of the identity of Ultimate Beneficial Owners (UBOs) if any.

Monitoring of Customers and Transactions

Ongoing monitoring of a business relationship includes:

- i) scrutiny of transactions to ensure they are consistent with our knowledge of the customer;
- ii) obtaining, where necessary, a source of funds and source of wealth; and
- iii) ensuring that documents, data, or information held are kept up-to-date.

PPBV conducts ongoing monitoring of customers' gambling habits and behaviours, to ensure that the transactions are consistent with the customer's risk profile. This includes analyzing customers' transactions in order to identify suspicious and/or fraudulent behaviour and unusual patterns which appear to have no valid economic purpose. A full audit trail of all transactions is maintained.

Internal Intelligence: All PPBV employees must be diligent and mindful of suspicious or unusual betting activity and/or transactions during their daily tasks and must not assume it is another person's responsibility to monitor or report such activity. All employees can raise internal suspicions through the following mechanisms:

- Through emailing
- In the event of staff feeling unable to raise suspicions through internal reporting channels, a Group-wide confidential reporting service is available. Such suspicions will be managed under the remit of this policy and also the PPBV Whistleblowing Policy.

External Intelligence: Negative media, regulatory, and police enquiries are utilized on an ongoing basis to identify higher-risk retail customers. Enhanced due diligence will be performed on customers identified through external intelligence and an external report will be considered by the Money Laundering Reporting Officer (MLRO) or delegate.

PEPs and Sanctions

Politically Exposed Persons (PEPs)

PEPs are individuals who are or have been entrusted with prominent public functions, for example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, and important political party officials. PEPs are considered "higher risk" because the positions that they hold can potentially be abused for private gain, corruption, bribery, or abusing or misappropriating public money. Similarly, relatives and close associates (RCAs) of PEPs can also benefit from, or be used to facilitate abuse by the PEP of their position and therefore enhanced due diligence measures are required on RCAs of PEPs.

The EDD measures required for PEPs and RCAs are:

- 1) Ensure approval from senior management is obtained before a business relationship is established with the customer, or where a customer becomes a PEP after the establishment of the business relationship, ensure approval from senior management is obtained to continue the relationship. For the avoidance of doubt, senior management means the Money Laundering Reporting Officer (MLRO) or a Deputy MLRO;
- 2) Determine the source of funds and the source of wealth of the customer (discussed further below).

To ensure PPBV is compliant with PEP requirements all customers are screened against PEP Lists on a regular basis.

Sanctions

Sanctions are imposed by Governments and international bodies such as the EU and UN and may apply to individuals, entities, and governments. PPBV will adhere to HMT, EU, UN, and OFAC (USA) sanctions regimes. To ensure PPBV is compliant with such sanctions regimes all customers are screened against Sanction Lists on a regular basis.

Enhanced Due Diligence

PPBV transactional and behavioural monitoring is achieved through the use of an array of manual and automated behavioural and monetary triggers. Should a customer meet the criteria for review; or be escalated to the AML team from any part of the business; an EDD review will be conducted.

The EDD process looks to establish additional information about the customer, with a particular focus on defining the customer's risk profile. As part of the EDD process, customers will be assessed through the AML EDD Risk Calculator and their risk score will determine the next actions to be taken. The AML EDD Risk calculator establishes a score based upon the customers' profiles and transaction history. The higher the score the higher the perceived customer risk and defines next steps, are as follows:

Risk Rating	(Minimum) Required Action
Low Risk	• Updated CDD documentation may be required
Medium Risk	• Updated CDD documentation may be required • Evidence of Source of Funds and Wealth required • Deadline of 8 weeks • Account limit applied until satisfactory documentation provided¹
High Risk	• Updated CDD documentation may be required • Evidence of Source of Funds and Wealth required • Deadline of 4 weeks • Account limit applied until satisfactory documentation provided¹
Urgent Action	• Updated CDD documentation may be required • Evidence of Source of Funds and Wealth required • Deadline of 1 week • Account limit applied until satisfactory documentation provided

Source of Funds and Source of Wealth

Source of Funds refers to the activity (e.g. occupation or business) generating the funds used in a particular transaction.

Source of Wealth is much broader and refers to all of the economic activities that have generated the customer's wealth, and can include for example income through employment or business, inheritance, or sale of property.

The extent of documentation requested will vary depending on the risk posed by the customer. In lower-risk situations PPBV may take less intrusive and less exhaustive steps to establish the source of funds and source of wealth of the customer such as publicly available information. In higher-risk situations, PPBV will not just rely on information provided by the customer but will require documentary evidence.

Source of Funds & Wealth Engagement

Customers presenting a medium or higher risk of money laundering / potentially using proceeds of crime will be engaged directly to establish the source of funds and wealth. This engagement will be conducted by the appropriate Relationship / Customer Service Manager and the customer will be asked to provide sufficient information (proof of income, assets owned, etc.) to give us comfort that their deposits are not the proceeds of crime.

In the event that a customer fails to provide an adequate source of funds and wealth within the agreed timeframe, the customer will be suspended and a decision to report to the relevant authorities will be considered. The decision to suspend and the decision to report are separate processes. A decision to suspend a customer will be taken by the AML team. Should an account be closed by the AML team, that customer can no longer be given access to our products or services until sufficient information is received to justify re-opening the account.

To reduce the risk of reputational damage, all offers of gifts & hospitality for high-value customers will be subject to AML & Responsible Gambling reviews before the gift or hospitality being offered. Please refer to the PPBV Gifts and Hospitality Policy for more information.

Reporting Suspicious Activity

All staff must raise an internal report where they have knowledge or suspicion, or where there are reasonable grounds for suspicion, that another person is engaged in money laundering:

- **Knowledge:** Having knowledge means knowing something to be true;
- **Suspicion:** Suspicion does not require firm evidence but must be based on objective observations or inconsistencies that warrant further investigation
- **Reasonable grounds for suspicion:** Reasonable grounds exist when a trained employee, based on known facts, would be expected to form a suspicion.

Having made a report, an employee should not indicate their suspicions to the customer or reveal that a report has been made; as such actions could constitute the criminal offense of “tipping off”, which is discussed further below.

Upon receipt of an Internal Suspicious Activity Report, the AML team will investigate the suspicion and will decide whether to submit a Suspicious Activity Report (SAR) to the appropriate Financial Intelligence Unit (FIU). Where a decision is made to submit a SAR to the appropriate FIU the AML team must do so as soon as is practicable after completing their investigation.

The decision to submit a Suspicious Activity Report to the appropriate Financial Intelligence Unit is the sole responsibility of the AML team (on behalf of the MLRO). All decisions will be made independently of operational processes.

Failure by a customer to provide the appropriate documentation and/or information for the purposes of verification of identity and/or source of wealth verification can be considered reasonable grounds for suspicion.

Any information request received from a regulator or police authority that explicitly notes or implies that a customer is involved in money laundering or criminal activity should be referred to the AML team without delay by email.

Record-Keeping Requirements

As detailed within the PPBV Data Retention Policy PPBV maintains records of all relevant transactions carried out by or on behalf of customers (such as records sufficient to identify the source and recipient of payments from which investigating authorities will be able to compile an audit trail for suspected money laundering or the financing of terrorism) for a minimum of 7 years from the date when the customer formally ceases to be a customer.

Records of information or documentation used to carry out CDD or EDD on a customer are maintained for a minimum period of 7 years from the date that the customer formally ceases to be a customer.

This minimum period is longer in some international jurisdictions but full details are available in the Data Retention Policy.

Training & Awareness

All PPBV staff are required to undergo annual AML/CFT Awareness training as part of the company's Compliance training program. Staff are tested as to their understanding of the training and the results recorded against each individual training record.

The annual training outlined above will be supplemented by role-based bespoke training for specific teams that are potentially more likely to encounter money laundering.

Roles & Responsibilities

It is the responsibility of the MLRO and Deputy MLRO to implement and manage anti-money laundering measures including internal policies, controls, and procedures, and to ensure that, when appropriate, information or any other matter leading to knowledge or suspicion or reasonable grounds for suspicion of money laundering is properly disclosed to the relevant authorities (as soon as is practicable).

Links Between AML and Responsible Gambling (RG)

The AML team will refer customers for whom there are any RG concerns to the RG Operations team.

Policy Approval

The Board of Directors has overall responsibility for ensuring that this policy complies with our legal and regulatory obligations and that all those under its scope comply with the requirements therein. The MLRO and Deputy MLRO through customer Relationship Managers have primary and day-to-day responsibility for implementing this policy. Management at all levels is responsible for ensuring those reporting to them are made aware of and understand this policy and operate within its guidelines. The MLRO is responsible for ensuring knowledge or suspicion, or reasonable grounds for suspicion of money laundering is properly disclosed to the relevant authorities (as soon as is practicable).

Appendix D – PPBV Compliance- Three Lines of Defense

The PPBV risk framework is based upon the Three Lines of Defense model to allow for structured roles, responsibilities, and accountabilities to be built into risk decision-making. The first line is business operations, with responsibility for ensuring a risk and control environment is established as part of day-to-day operations. The second line is oversight functions (e.g. Compliance), with responsibility for setting company boundaries by drafting and implementing policies and procedures within risk appetites. The third line is independent assurance providers such as Internal Audit, who provide objective assurance activities designed to improve the company's operations. The graphic below further outlines the risk framework adopted across Paddy Power.

