

AML/CTF Policy

| Name | Description |
|-------------------|--|
| Document Name | Customer Interaction Manual |
| Version | 3.0 |
| Author | Victoria Knight– Compliance Department |
| Authorised By | Greg Knight – Managing Director |
| Distribution Date | October 2022 |
| Review Date | October 2023 |

Policy Statement

All gambling operators have a responsibility to work towards keeping financial crime out of gambling. Legislation, regulation and guidance place an obligation on operators to be alert to customer attempts to gamble with the proceeds of crime. This includes both the act of using criminal proceeds to fund gambling, or by extension, attempting to obtain legitimate or 'clean' money in return.

A risk-based approach is required, with risk-based rules and criteria to proportionately manage Money Laundering ("ML") and Terrorist Financing ("TF") risk. At the Jenningsbet group, Jennings Racing Ltd, Jennings Racing (2006) Ltd, Betting Shop Operations Ltd and Joe Jennings Bookmakers Ltd, we are committed to preventing Money Laundering (ML) and Terrorist Financing (TF) being facilitated under the brand 'Jenningsbet' (collectively referred to as 'Company', 'we', 'us' or 'our' in this policy).

The purpose of this Policy is to reasonably address the responsibilities of the Company and its staff in relation to these obligations. Our AML/CTF policy, procedure and controls sits within the Compliance Team's 'plan, do, check, act, evaluate' framework and is therefore continually reviewed. At the minimum this policy is reviewed annually.

Scope of policy

Mitigating against ML/TF requires the full commitment and support of senior management, and the active co-operation of all employees. This policy applies to all individuals working for or on behalf of the Company at all levels and grades, whether permanent, fixed-term or temporary, and wherever located, including consultants, contractors, seconded staff, casual staff, agency staff, and any other person who performs services for or on behalf of the Company.

The outcome sought from this policy is that:

- We meet anti-money laundering legal requirements and associated regulations
- Staff are aware of and understand the AML legal requirements, offences and background set down in this policy – and appropriate support is in place to ensure it is complied with
- We have a robust, risk-based process that is effectively and consistently followed, to understand with whom we are dealing and any money laundering risks
- Money laundering suspicions are proactively and immediately reported
- We maintain comprehensive records of anti-money laundering checks and concerns

This Policy should be read with all other pertinent Jenningsbet Policies.

Money Laundering

All gambling operators have a responsibility to work towards keeping financial crime out of gambling. Legislation, regulation and guidance place an obligation on operators to be alert to customer attempts to gamble with the proceeds of crime. This includes both the act of using criminal proceeds to fund gambling, or by extension, attempting to obtain legitimate or 'clean' money in return.

The key objectives for money launderers are to:

- Disguise the source of criminal property;
- Conceal / distance ownership of criminal property but still keep control of it;
- Avoid detection for the underlying crimes; and
- Benefit from the proceeds of crime securely.

Money laundering may take a variety of forms and use a number of methods using all financial services and products. Traditionally the money laundering process comprises three main stages:

1. Placement – where funds from criminal activity are placed into the financial system. For Jenningsbet this would be at the point of customer payment;
2. Layering – Which usually involves a complex system of transactions designed to hide the source and ownership of the funds, and to confuse authorities. For Jenningsbet this could for example relate to customers betting equally on red and black on roulette
3. Integration – where laundered funds are reintroduced into a legitimate economy, appearing to have come from a legitimate source. For Jenningsbet this would be when customers have returns on their bank account.

Terrorist Financing

Terrorist financing is a general term to describe activity that provides or facilitates the provision of money or property to be used for terrorist purposes.

Traditionally AML efforts have concentrated on the criminalisation of the laundering of the proceeds of different forms of underlying criminal conduct. Terrorist financing is a serious threat to financial businesses or businesses where a high volume of monetary transactions take place. This threat must be taken as seriously as money laundering.

The mainstream methods to raise funds used by terrorist organisations include: -

- Private donations by terrorist supporters / sympathisers
- Abuse and misuse of non-profit organisations and charities
- Criminal activity
- Legitimate commercial activity

Terrorist financing often involves a complex series of transactions; like money laundering, this generally follows three separate phases: -

1. Collection – funds are often acquired through seeking donations, carrying out criminal acts, or diverting funds from genuine charities.
2. Transmission – where funds are pooled and transferred to a terrorist or terrorist group.
3. Use – where the funds are used to finance terrorist acts, training, materials, accommodation, propaganda, etc.

However, like three stage model of money laundering, this model is fairly simplistic and outdated, so it is important not to get caught up in trying to determine if an activity follows this pattern; instead, focus on whether you have *knowledge, suspicion, or reasonable grounds to suspect*.

Common Factors: Money Laundering and Terrorist Financing

Factors in common are:

- Laundered proceeds may eventually fund future or prospective criminal acts;
- The *destination* of money used to support terrorism has to be disguised in the same way that the *source* of laundered funds must also be disguised;
- Even where the source of funding for terrorist activity is lawful, terrorists will still attempt to disguise it in order to preserve the future funding stream

AML/CTF Company Reporting Structure

The below structure sets out the reporting and communication flows between departments in the AML/CTF organisational chart.



AML Organisational Chart

Core Responsibilities

Directors

The Director of the Company Greg Knight approves AML/CTF Policies and other AML-related manuals, at least annually, or when required. He is responsible for ensuring this policy is adhered to and there is sufficient resource to ensure it can be adhered to. The Board and Head of Compliance will review AML/TCF matters at monthly meetings.

Head of Compliance:

The Head of Compliance is responsible for the drafting and any subsequent changes in the AML/CTF for the Company this is done annually at a minimum. The Head of Compliance will ensure staff in the

departments shown in the AML organisational chart are aware of this policy and its requirements – and have the knowledge and skills to implement it. They will also hold a Gambling Commission Personal Management Licence for Regulatory Compliance and the role of the companies Money Laundering Reporting Officer (MLRO). They have ownership of the Compliance Team’s ‘plan, do, check, act, evaluate’ framework that this policy sits within.

Definitions

Money Laundering (ML): The process of concealing the origins of money obtained illegally by passing it through a complex sequence of banking transfers or commercial transactions.

Terrorist Financing (TF): the movement of funds through the financial system with the intention of funding terrorists or terrorist acts. To remain “under the radar,” similar to other criminals, terrorist organizations must disguise the origins of their funds to remain undetected.

Suspicious Transaction: A transaction for which there are reasonable grounds to suspect that the transaction is related to a Money Laundering offense or a Terrorist Financing offense.

Betting: is the making or accepting a bet on (a) the outcome of a race, competition or other event or process, (b) the likelihood of anything occurring or not occurring, or (c) whether anything is or is not true. For the purpose of Gambling Commission regulation, a "bet" does not include a bet the making or accepting of which is a regulated activity within the meaning of section 22 of the Financial Services and Markets Act 2000

Over The Counter (OTC): A product that is betting in a betting premises (mainly sports betting) which is not gaming machines betting.

Self-Service Betting Terminal (SSBTs): OTC betting products that are placed on a terminal

Gaming Machines (GM): a machine which is designed or adapted for use by individuals to gamble including Fixed Odds Betting Terminals (FOBT)

SARs– A suspicious activity report (SAR) is a disclosure made to the National Crime Agency (NCA) about known or suspected: money laundering – under part 7 of the Proceeds of Crime Act 2002 (POCA) terrorist financing – under part 3 of the Terrorism Act 2000

Smurfing: Customer will break up large transactions into a set of smaller transactions that are each below the reporting threshold to avoid suspicion.

Closed loop: payment to the customer is made on the same method that was used by the customer to deposit funds. This being cash to cash or card to the same card.

KYC: The process used to establish the identity of a customer to ensure the individual has obtained their funds legally and that they are sustainable relating to level of spend.

Proceeds of Crime: property from which a person benefits directly or indirectly, by being party to criminal activity i.e. stolen money, money from drug dealing, tax evasion or stolen, thieved or robbed property. It includes property that a person gains by spending the proceeds of criminal activity, for example, if a person used money gained in a bank robbery to gamble

PTL: *'Permission to Lay'* process involves an assessment from Raceroom staff to manage betting liabilities and bet acceptance taking into account trading and AML/CTF risk.

BGC: Industry trade association *'Betting and Gaming Council'*

Regulatory Requirements

products.

Jenningsbet ensures that such policies, procedures and processes are robust, updated and communicated to all staff where appropriate. Ongoing monitoring and compliance take place to provide assurance to the Director and the regulators that Jenningsbet continues to meet its obligations under relevant legislation, including: -

- Gambling Act 2005
- Proceeds of Crime Act 2002
- Terrorism Acts 2000 and 2006
- Gambling (Licensing and Advertising) Act 2014
- Gambling Commission's guidance on the prevention of money laundering and combating the financing of terrorism, Fifth Edition (Feb 2021)
- Sanction and Anti-Money Laundering Act 2018
- Licence Conditions and Codes of Practice
- Sanctions and Anti-Money Laundering Act 2018 (SAMLA)

Gambling Act 2005

The 2005 Act sets out the following three objectives for operators:

- Preventing gambling from being:
 - a source of crime and/or disorder;
 - associated with crime and/or disorder; or
 - used to support crime
- Ensuring that gambling is conducted in a fair and open way.
- Protecting children and other vulnerable persons from being harmed or exploited by gambling.

The Act is enforced by the Gambling Commission and Licensing Authorities, which are local authorities operating through Licensing Committees. The Commission's set out their requirements in their Licensing Conditions and Codes of Practice (LCCP).

Proceeds of Crime Act 2002 (POCA)

POCA creates several principal offences that apply to everyone and criminalise any involvement in the proceeds of any crime if the person knows or suspects that the property is criminal property. 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. 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. Particular attention should be drawn to the below sections of POCA:

1. Section 327 states that a person commits an offence if they conceal, disguise, convert, or transfer criminal property in the UK. Converting may take the form of a customer placing a bet and cashing in the winnings, while concealment may involve placing money into a betting terminal and not using it may be indicative of the concealment, disguise and transfer of funds.
2. Section 328 provides that a person commits an offence if he or she enters into or becomes concerned in an arrangement which he or she knows or suspects facilitates, by whatever means, the acquisition, retention, use or control of criminal property to or on behalf of another person. This may occur where a shop accepts stakes which are known or suspected to be the Proceeds of Crime (POC).
3. Section 329 states that a person commits an offence if he or she acquires, uses, or has possession of criminal property. As above, this could involve the use of criminal proceeds from, for example, a burglary, to place a bet with Jenningsbet.
4. Section 342 states that to disclose knowledge of the existence of any investigation prior to or following a report which could prejudice the investigation' (this is often related to as 'tipping off' though this is not to be confused with the actual offence of tipping off which is only an offence in the regulated sector). The penalty upon conviction is a maximum of 5 years imprisonment.

Jenningsbet are also obligated to follow any advice published by our regulators relating to POCA or any applicable statutes. This includes the GC published document 'Duties and responsibilities under the Proceeds of Crime Act 2002 (November 2002).

Terrorism Act 2000 (TACT)

Jenningsbet have obligations under the Terrorism Act (TACT) This defines the primary offences related to terrorist funding and requires regulated businesses to report knowledge or suspicion of offences. Under section 18 of the act A person commits an offence if he enters into or becomes concerned in an arrangement which facilitates the retention or control by or on behalf of another person of terrorist property.

Penalties

The above offences can be committed by any person, including employees who have knowledge or suspicion that a customer is using the POC. The penalty upon conviction of these sections is a maximum term of 14 years imprisonment, a fine, or both. You should note that offences can be committed by staff as individuals even if you are acting in the course of your employment.

Defences

There are certain defences available for some of the offences listed above including the defence of having made an 'authorised disclosure' before any offence is committed.

If a disclosure is made to the MLRO then that disclosure will be sufficient for a staff member to rely on this defence, provided they disclose before any offence has been committed.

Note that if the MLRO does report any suspicions to the NCA staff must discuss with the MLRO what information should be given to the customer, so that the offence of tipping off is not committed.

Risk Assessment

The retail gambling sector benefits from consistent customer-focused innovation. However such innovation bring new risks requires our processes to remain robust so we are able to identify and manage these risks. This policy should be read in conjunction with our AML Risk Assessment which sets out in detail our identified risks and their RAG status.

It is important to note that HM Treasury's National Risk Assessment rated the Gambling Sector as low risk. When gambling is put into the wider financial context of being vulnerable to money laundering and terrorist financing in comparison to other regulated sectors such as banking, the risk is lower; thereby explaining HM Treasury's rationale for rating gambling as low risk for ML and TF.

Training

Our employee training forms as a primary control against the majority of the ML/TF risks. Staff in all the teams shown in the AML organisational chart are trained on the regulatory framework Jennings operates in with emphasis on their individual responsibilities and accountability. The training programme covers: what money laundering is and what incidents they may detect that could constitute money laundering, to whom suspicious cases should be reported and the role of Money Laundering Reporting Officer.

The training of all staff annually on AML is a requirement set out in the GC's LCCP and records of all staff training is kept with the training department. The AML training programme is the responsibility of the Head of Compliance who will approve all training materials and is responsible for ensuring the LCCP requirement is met. Ensuring all training record-keeping is in line with Data Protection obligations is the responsibility of the Head of Compliance.

Gambling Related Harm

It is acknowledged that some risk indicators may be indicative of money laundering, terrorist financing but also equally problem gambling (or both). These risk indications commonly are:

- Customers who bet with funds that are known to be outside of their means
- Changes in a customers' betting or gaming level. Dramatic increases with no indication of the source of funds
- Notification that a customer has been excluded (this could be via self-exclusion in relation to prevention of harm) or asked to provide source of funds information by a competitor on the basis of risk triggers.

- Funding bets with one payment method and requesting for funds to be returned to a different method, for example, betting in cash and asking for funds to be returned to debit card or via bank transfer.
- Attempting to use someone else's card for payment.

We mitigate against the risk of problem gambling within our social responsibility framework and have robust measures in place to prevent gambling related harm.

Jenningsbet remain curious as to the source of customer funds and conduct ongoing customer monitoring to ensure that customer spending levels align with our knowledge of their affordability to gamble.

Customer Monitoring

No system of checks will detect and prevent all money laundering activity. A risk-based approach involves a realistic assessment of the threat of Jenningsbet being involved, albeit unintentionally, in money laundering. It focuses the effort where it is most needed and will have the most impact. In order to detect customer activity that may be suspicious, it is necessary to monitor all transactions and customer activity including spend and behaviour using a risk-based approach.

Jenningsbet have considered a wealth of information and intelligence when implementing customer monitoring controls that are robust, fit for purpose and risk-based. These have been compiled using shared industry learnings through the BGC retail working group and collaboration with GAMLG (The Gambling Anti-Money Laundering Group).

Money Laundering Reporting Officer

MLRO

Peter Jowett is the Money Laundering Reporting Officer (MLRO). He is available on 07764 897030 or peter.jowett@jenningsbet.com.

Where it is known or suspected that money laundering may be taking place, such knowledge or suspicion must be reported immediately to the MLRO and the customers' business should not be accepted unless the MLRO gives their specific consent.

SARs

Suspicious Activity Reports (SARs) alert law enforcement to potential instances of money laundering or terrorist financing. They provide information and intelligence from the private sector that would otherwise not be visible to law enforcement.

Persons working in the regulated sector are required under Part 7 of POCA and TACT to submit a SAR in respect of information that comes to them in the course of their business if they know, or suspect or have reasonable grounds for knowing or suspecting, that a person is engaged in, or attempting, money laundering or terrorist financing. By submitting a SAR to the NCA we are complying with our obligations to report suspicious activity.

The MLRO will decide whether to report the suspicion to the NCA in the form of a Suspicious Activity Report. Responsibility of this reporting sits with the MLRO. They must decide whether to submit the

SAR under either POCA or TACT, depending on the nature of the knowledge or suspicion and on a case by case basis. Where a suspicion is reported, the MLRO should wait until a response is received from the NCA. Where a 'refusal to proceed' is received there is a further period of 31 days for the NCA to follow up their refusal with further instructions

PEP and Sanctions

Part of this risk-based approach is ensuring customers are not persons on HM Treasury's sanctions list or a Politically Exposed Person (PEP). A PEP/ sanctions search is part of our KYC requirements detailed in our AML Procedures and Controls document.

Maintaining records

Any information obtained in our AML KYC procedures will be stored in line with Data Protection requirements. If necessary under our legal obligations such data will be provided to regulatory authorities and public bodies namely the Gambling Commission, HMRC, Police and the National Crime Agency (NCA). All monitored customer data is stored and retained for a period of 7 years and then destroyed.

External Audit

Jenningsbet use a third party to audit our AML policies, procedures and controls namely MCH Services.