October 2022

AML/CTF Procedures and Controls for Jenningsbet Branches

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

Introduction

Gambling is a legitimate activity, but it can also present opportunities for crime. This document will outline the procedures and controls we have implemented at Jenningsbet in our branches in order to uphold the Company's responsibility to keep financial crime out of gambling.

We remain committed to ensuring that criminals cannot launder the proceeds of crime through Jenningsbet products or services. We continue to scrutinise abnormal customer betting activities in order to assess risk and spot gambling-related crime. Whilst some relationships with customers will be transient or temporary in nature, consideration to this issue in relation to all customers is given.

Preventing Money Laundering (ML) and Terrorist Funding (TF) requires clear communication of the policies, procedures and controls to all employees, along with robust mechanisms to ensure that they are carried out effectively, weaknesses are identified and improvements are made, wherever necessary. This document should be read in conjunction with our AML Risk Assessment and AML Policy.

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.*

Smurfing: C*ustomer 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*

Money Laundering Detection

No system of checks will detect and prevent all ML/TF activity. A risk-based approach will focus 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.

Customer Activity is monitored day to day by the shop team. Staff are trained to spot the signs of ML/TF and the escalation processes. These signs include but are not limited to:

- Customer's bet characteristics (short prices, late bets, betting on all selections)
- Big changes in betting behaviour
- Customers payment methods
- Wanting receipts
- Suspicious Activity Alerts
- Local knowledge
- Intelligence from other Jenningsbet branches or competitors

It is important to note that some signs of ML/TF can be signs of gambling related harm. This document should be read in conjunction with our Customer Interaction Policy for more information.

Reporting Concerns

Customers

Being suspicious of a transaction does not require knowledge of the exact nature of the criminal offence or that the funds are definitely those arising from the crime.

Concerns or suspicions in regards to ML/TF about a customer should be made to the MLRO/Deputy MLRO. This concern should be raised in writing or, in the event of a call, will be formally recorded by the MLRO/deputy MLRO. Concerns can be raised by shop teams using the SR log, phone or email. You should use the SR log to record all Compliance related incidents including Age Verification Checks, Complaints, Customer Safer Gambling Interactions and Self Exclusion data.

Peter Jowett - MLRO – peter.jowett@jenningsbet.com 07764897030

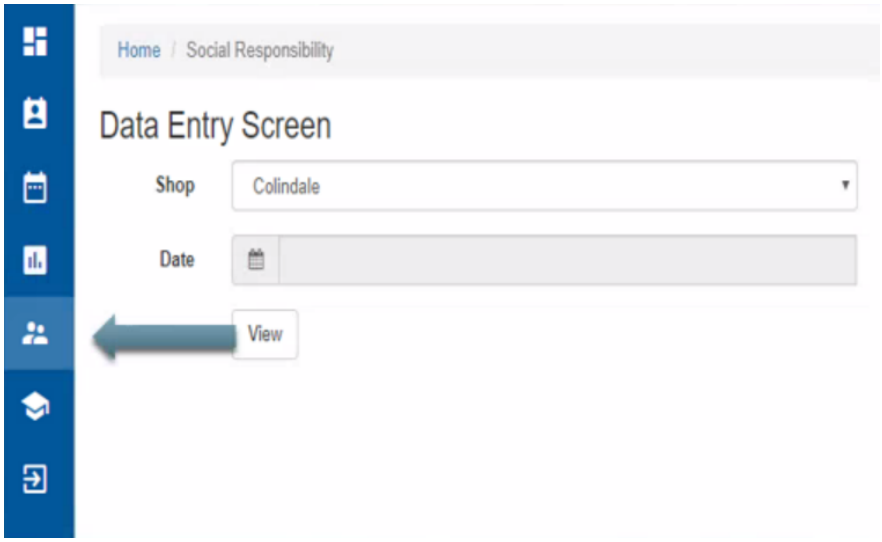
Craig Hagarty- Deputy MLRO – contentmanager@jenningsbet.com 07931538733

Vicky Knight Head of Safer Gambling vicky.knight@jenningsbet.com 07762275975

Raceroom – raceroom@jenningsbet.com 01992 574221

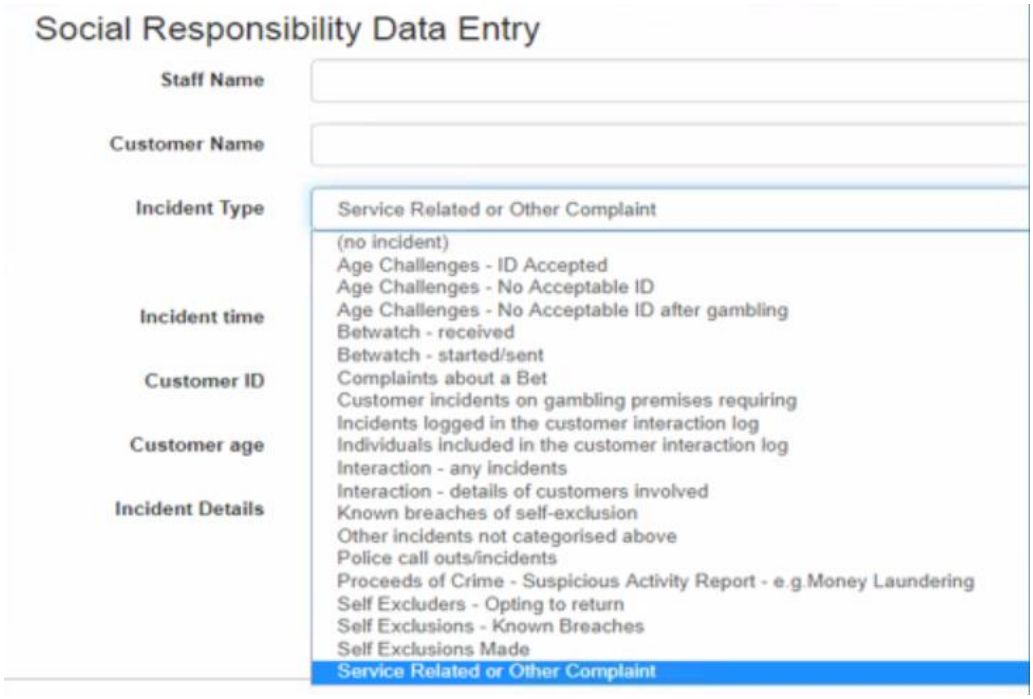
The below steps set out how to record incidents on the SR log.

Firstly select the Data Entry screen. This will be the shop you are currently working in will automatically be selected under 'Team' and the 'Date' will match the day you are recording the incident.



Once selected you can fill out the data entry points. If you are recording an ML/TF concern select 'Proceeds of Crime – Suspicious Activity Report' from the drop down menu. It's important to include all key information if you can including:

- Date/time
- Customer name if known
- What aroused suspicion
- If any conversations have taken place and with whom



Escalating Concerns

You can escalate suspicious activity or concerns directly with the Compliance Team via telephone or email as well as reporting on the SR log. Should you require an immediate response it is best to contact the Raceroom outside of office hours.

Once you have raised a suspicion you must not tell the customer you have reported them or discuss with anyone else. Remember that this is a legal obligation, if the case gets investigated it is a crime if you falsify, destroy or dispose of any information concerned with the case.

Any raised concern or suspicion is considered by the MLRO, in the light of all other relevant information available, to determine whether or not it gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that a person is engaged in ML/TF.

The MLRO will decide when a customer is assessed as presenting a higher risk and will decide when additional information in respect of that customer should be collected. Deciding that a customer presents a higher risk of money laundering does not automatically mean that the person is a criminal or is laundering money. Similarly, identifying a customer as having a low risk of money laundering does not mean that the customer is definitely not laundering money or engaging in criminal spend.

Colleagues

Concern or suspicion can be regarding colleagues as well as customers. If you have a concern regarding ML/TF in regards to a colleague this concern should be raised to the MLRO/Deputy MLRO. This should be in writing or via the telephone. A concern about a colleague should **never** be raised on the SR log. Reference should be made to our Whistleblowing policy for further clarity and guidance.

Customer Profiles

Raceroom and the Compliance Team will have customer profiles for those that have been identified usually through the SR log or monitored customers list.

Raceroom work with the shop teams to decide what customers to monitor for trading risk and PTL authorisation is required from the Raceroom team.

Customer profiles will include customer's status (i.e. new or established customer) and win/loss levels. Profiles are created for any customer staking £500 in a single bet OTC, or otherwise placing OTC bets to a value of £5,000 or more within a consecutive 3 day period. As well as for any customer loading £1000 onto an EGM in a single day, or otherwise loading credit to the value of £5,000 or more within a consecutive 7 day period.

Monitored customers are given a profile on the shop till system. The profile will include a 'Nom De Plume' (or real name if known), stakes, returns and bets.

The Compliance Team work in partnership with the Raceroom for Customer Reviews and evaluation.

Payment Methods

Suspicion should be aroused should a customer request anything outside of our normal payment procedures. This includes customers presenting any 'codes' to proceed with payment on the PDQ that they may claim are from a bank/card provider. Innovation in payment systems can cause confusion

around how to customers can pay/be paid so please remain vigilant and ring Raceroom if you are concerned. Customer's cannot pay using credit cards.

Please check that the customer's name on the card used to pay with matches the name used for any refunds (winnings) processed. The card name should also be their own.

Payment methods should follow a closed-loop system i.e cash/cash and card/card and no receipts are to be given.

All card refunds (winnings) over £8,000 should be made via the Raceroom and Finance team who will process as a bank transfer rather than being made back on the card. You should ensure that the customer's bank details taken from the card are emailed only to appropriate persons such as the Raceroom and Finance Team for payment. The sent emails from the shop containing the customer's details for bank transfer will automatically be deleted after an appropriate period in line with Data Protection laws.

Should a customer request any payment method or receipts outside of these norms then this should be made directly to the Raceroom who can communicate with the Compliance and Finance Teams.

Suspicious Activity Alerts

Suspicious Activity Alerts are triggered if a customer's play is suspected ML/TF. A Suspicious Activity notification will alert you via the terminal back-office behind the counter. You should then contact the Security Team for pay-out approval.

Dye Stained Money (DSM)

Money that has become stained by coloured dye or damaged by glue will have been obtained via a Cash In Transit (CIT) robbery. The dye and glue are released upon the unauthorised opening of the relevant cash boxes. Therefore, this is money that has been stolen and is considered criminal property.

Under no circumstances are you able to accept payment for bets by customers presenting DSM. If presented, by a customer, it must be refused and security advised immediately. Any instance must be recorded and logged on the SR log with an approximate time the customer attempted to present the DSM.

Should any amount of DSM be found following the emptying of either the Gaming Machines (FOBTs) or the Self Service Betting Terminals (SSBT), the Company has a legal obligation to inform the appropriate authorities.

Therefore, following procedure MUST be adhered to:

1: Ring the Security Team and advise accordingly.

2: Immediately separate the DSM from the other notes taking as much care as possible when handling the DSM. **(It is imperative that the notes are handled as little as possible)**

3: Make a note of the DSM values, i.e. 4 x £20 + 8 x £10.

4: Place the DSM in a sealed envelope and place in the shops safe.

5: Make a note of the terminal that the DSM was found within.

6: Book the value of the DSM as a shortage.

7: Once the above actions are completed, please email the MLRO and Security Teams providing details as above and record on the SR log.

8: Under no circumstances should any DSM notes attempt to be banked or returned to a customer.

Customer Verification

The Compliance Team will organise any ID requests directly to the customer either via written request directly or written request given to the customer via the shop team. When passing this request on you should also present the customer with a Jenningsbet branded leaflet explaining our obligations.

The ID should certified by yourself or the Compliance Team as appropriate to state that it is the customer in question and signed stating it is a true copy of the original. You should sign your name alongside the wording "Certified to be a true copy of the original seen by me".

The Compliance Team will verify the ID once received and will communicate to the shop team if the customer has satisfied the requests. The customer cannot bet with us until this authorisation has taken place.

Further KYC information may be requested at that point or at any stage in the relationship with the customer by the Compliance Team. Again this will be directly to the customer either via written request directly or written request given to the customer via the shop team following the same steps as the initial request.

Customer Review Outcomes

The Compliance Team will communicate to the shop and the customer any outcome of the KYC checks. These outcomes being: continued betting permitted, further review needed or business terminated. The Compliance Team will discuss these steps and how this will be communicated to the customer with the shop team on a case by case basis.

Training

Our employee training forms as a primary control against the majority of the ML/TF risks. Every member of the shop team is trained on the regulatory framework Jennings operates in with emphasis on individual responsibilities and accountability. The training programme covers: what money laundering is and what incidents they may detect that could constitute money laundering, our controls and to reporting/escalation procedures.

Training takes the form of face-to-face workshops upon induction and yearly online refresher courses. Updated AML Policy and AML Procedures and Controls documents are read as part of staff's required training. Should new risks be identified and felt to warrant more face-to-face training these are delivered on an ad-hoc basis. Should you feel you require more training on this or you haven't had the required training for any reason please alert the compliance team.

The latest AML policy and AML Procedures and Controls documents are on your online staff portal for reference.

MLRO

The MLRO monitors the day-to-day operation of AML and CTF policies and respond promptly to any reasonable request for information made by the GC or law enforcement bodies. The MLRO takes ultimate managerial responsibility for AML issues, but this does not diminish senior management responsibility for AML.

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. Should the MLRO be absent from the business for any reason such as annual leave; they will communicate the date and time to all employees via email and explain that the deputy MLRO should be contacted. Should the MLRO be unable to communicate this in advance for example if they fall ill then the deputy MLRO will communicate that they are acting MLRO temporarily. A register is kept by the Compliance Team of the handovers of the responsibility with dates and times set out.

Whilst disclosure to another of the fact that a person may be engaged in money laundering is generally an offence, such disclosures to a MLRO are specifically protected, where they are made as soon as is practicable and the information came to their attention in the course of their employment. Whilst reporting any suspicions to the MLRO, staff must also continue to be aware of the tipping off offence that is that it to disclose knowledge of the existence of any investigation prior to or following a report which could prejudice the investigation.

If an employee makes a disclosure to our MLRO then that disclosure will be sufficient for them to rely on as defence, provided it is disclosed before any offence has been committed.

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. The Responsibility of this data storage sits with Peter Jowett.