June 2022

AML Risk Assessment

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

June 2022

Introduction

Gambling is a legitimate activity, but it can also present opportunities for crime. This document will outline the regulatory requirements and current risks of Money Laundering (ML) and Terrorist Financing (TF) for Jenningsbet. The retail betting landscape is ever-changing, with constant innovation and an increased and more complex range of services. There is enhanced ability to accept a greater number of payment methods and improve customer experience. These changes bring new risks and it is therefore imperative that our Anti Money Laundering (AML) processes remain robust and we are able to identify and manage these risks.

In relation to the Gambling sector currently, only remote and non-remote casinos are subject to the Money Laundering Regulations (MLRs), with all 'other gambling' including Jenningsbet as an off-line off-course operator subject to the Gambling Act 2005 regulations.

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 Licencing Conditions and Codes of Practice (LCCP). Jenningsbet also have legal duties under the Proceeds of Crime Act 2002 (POCA) and the Terrorism Act 2000 (TACT) to help mitigate against financial crime.

The purpose of this document is to make clear and accessible the ML and TF risks we have identified, the level of risk we have given these and controls or treatments to risk we have implemented. These are in line with our risk tolerance level and risks are reassessed post mitigation.

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)*

Smurfing: C*ustomer will break up large transactions into a set of smaller transactions that are each below the reporting threshold to avoid suspicion. They may deploy 'smurfs' to do these for them to hide connection even futher. Such money can then be legalised through transfer to a bank account. The 'smurfs' are careful to deal with amounts below the legal monetary thresholds.*

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'*

Organised Criminal Gangs (OCGs): are using multiple land based betting premises to place bets with funds that have been derived from the proceeds of crime.

'Bring your own devices' (BYODs): There is the technology available for customers to use their own device (for example, mobile phone) to place bets through non-account based play either in off-course or on-course venues.

Methodology

At Jenningsbet we operate a 'plan, do, check, evaluate, act' framework. This helps facilitate a continuous cycle of improvement. The Compliance Team carry out ongoing horizon scanning and include new identified risks for Jennings as a Betting Operator (offline, off-course) in the Risk Assessment as appropriate.

This cyclical framework involves collaboration with other relevant departments, senior management and Directors particularly to identify new product risk. Jenningsbet have an active role within our trade

association the Betting and Gaming Council (BGC) and sit on numerous working groups that encourage shared industry data and learnings.

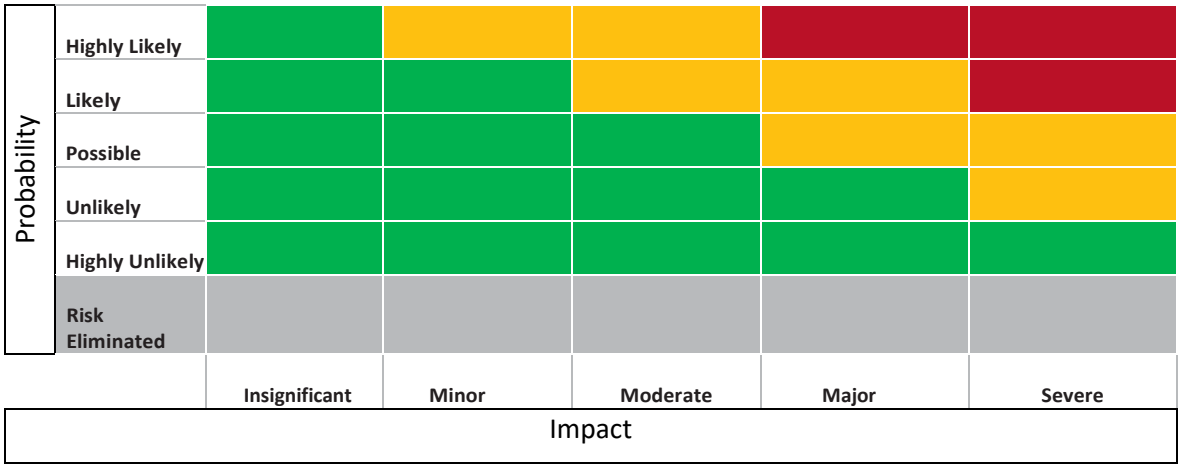
Jenningsbet have therefore considered a wealth of information and intelligence when assessing the key threats identified within the sector in consultation with in-house and external subject matter experts. We have also analysed information from various other sources to inform our understanding of risks such as:

- HM Treasury National Risk Assessment of Money Laundering and Terrorist Financing 2020
- The Gambling Commission The Money Laundering and Terrorist Financing Risks Within The British Gambling Industry November 2020
- The Gambling Commission The Money Laundering and Terrorist Financing Risks Within The British Gambling Industry November 2017
- Gambling Anti Money Laundering Group (GAMLG) AML Risk Assessment For Licensed Betting Offices and Remote Gambling Industries (LBOs) 2017
- FATF Standards

Once risks are identified a risk-based approach is applied; therefore focusing effort where it is most needed and will have the most impact.

This risk assessment has categorised our ML and TF risks as either payment risk, customer risk, employee risk, product risk and other risk although naturally there is a crossover. These have been assessed on both probability and impact.

In order to calculate the total risk level of red, amber and green, the probability and impact relationship levels are assessed in relation to each other. These determine the control measures we have put in place in line within our risk tolerance. The table below demonstrates how we arrived at our RAG status for each risk type.



From there we design procedures and controls to manage and mitigate the risks and give a risk rating for each separate risk post risk treatment.

Jenningsbet then monitor the efficiency of these controls taking into account new risks and changes in likihood and probability as a continuous cycle.

This document should be read in conjunction with our AML Policy and Procedures and Controls.

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.

It is acknowledged that some risk indicators (for example increasing customer spend or activity inconsistent with the customer's profile) may be indicative of money laundering, terrorist financing but also equally problem gambling (or both). We mitigate against the risk of problem gambling within our social responsibility framework and have robust measures in place to prevent gambling related harm.

Changes from previous version

There has been an increase in the risk levels for some of the inherent risks for the non-remote betting sector.

- **Vulnerabilities in the closed loop system** - the pandemic has seen an increase in cashless payments. There is the risk not operating a 'closed loop' system i.e., payment to the customer is made on the same card that was used by the customer to deposit funds. This coupled with the increased evidence the Commission is seeing of card fraud or theft means that operators should implement effective policies, procedures and controls involving a 'closed loop system'. The commission have given this a high risk rating. Customer returns should, other than in specific risk based exceptions, be sent back to the same source where the money funding the bet originated (in effect forming a 'closed loop') i.e card to card, cash to cash. However there is sometimes difficulty with this as certain banks namely Santander and Natwest not currently allowing returns via Mastercard. In these cases money is sent to customers bank account as a manual process set up by the finance team. This is still a relatively small amount of incidents and a resolution is being worked on with Mastercard.

- **Emerging Risk Pre-paid cards**. 'Smurfing' (using pre-paid cards) has been known to be used to fund terrorist activities. Here criminals can employ people ('smurfs') to purchase pre-paid cards which are then loaded with illicit money including Scottish notes. Such money can then be legalised through transfer to a bank account. Due to current limited evidence levels this has been given an overall low risk rating.

- **Organised Criminal Gangs (OCGs)** are using multiple land based betting premises to place bets with funds that have been derived from the proceeds of crime. The Gambling Commission has been given a medium risk rating. This has been incorporated under our 'Runners' and 'Customers using multiple branches' categories.

- **'Bring your own devices' (BYODs)** There is the technology available for customers to use their own mobile phone to pay using the 'wallet'. Risk of customers betting through credit cards through a 'wallet' solution.

- Note – Contactless payment cap increased to £100

Area		Risk	RAG Status	Definition	Risk Controls	RAG Status Post Control
Payment Risk	1	Dye Stained Bank Notes		Criminals target betting shops in an attempt to launder bank notes that have been permanently stained by cash degradation dye released during Cash In Transit (CIT) robbery. Notes can be inserted into gaming machines to obtain clean notes via payment at the counter.	Gaming Machines sensors offer complete note image capture to authenticate the validity of notes. Gaming Machines will give a security warning to staff. When used in conjunction with CCTV, can be used to identify customers suspected of money laundering and offer law enforcement an audit trail	
	2	Cash Betting		Criminals using cash representing the proceeds of crime may convert the criminal funds into legitimate funds.	Customer returns should, other than in specific risk based exceptions, be sent back to the same source where the money funding the bet originated (in effect forming a 'closed loop') i.e card to card, cash to cash. However present risks to the closed loop system outlined above.	
	3	'Smurfing'		Customer will break up large transactions that may be the proceeds of crime into a set of smaller transactions that are each below the reporting threshold to avoid suspicion.	All bets are monitored and patterns and trends identified on bets within a localised area by Race Room.	
	4	Cashless Betting		Commission seeing increased evidence of cashless betting from the pandemic and increased card fraud or theft, there is also the increased risk of 'smurfing' with cashless betting.	The closed loop system helps mitigate against this as well as the limit placed on contactless transactions (currently maximum of £100). However present risks to the closed loop system outlined above.	
	5	Requests to Pay Out Winnings Via Different Payment Methods		Criminals using cash representing the proceeds of crime may convert the criminal funds into legitimate funds.	Customer returns should, other than in specific risk based exceptions, be sent back to the same source where the money funding the bet originated (in effect forming a 'closed loop') i.e card to card, cash to cash. There is sometimes	

					difficulty with this as certain banks namely Santander and Natwest not allowing returns. In these cases money is sent to customers bank account.	
	6	Use of Shop To Withdraw Online Funds From Jenningsbet.com		Criminals using cash representing the proceeds of crime may convert the criminal funds into legitimate funds.	Customer returns should, other than in specific risk based exceptions, be sent back to the same source where the money funding the bet originated (in effect forming a 'closed loop') i.e card to card, cash to cash. Close communication protocols between Jenningsbet online and retail compliance teams.	
	7	Scottish Notes		There are no Jenningsbet branches in Scotland itself or near the border so customers attempting to provide large quantities of Scottish notes to place their bets may have ML vulnerabilities.	Jenningsbet have an escalation procedure in place should staff find customers attempting to use large quantities of Scottish notes	
	8	Pre Paid Cards		Criminals using cash representing the proceeds of crime may convert the criminal funds into legitimate funds.	Continuous working with our payment provider for possible solutions	
	9	Forced Payment Code		Customers can present a 6 digit code that can force a transaction through that otherwise declines. Code is from there phone and staff think is a bank issue.	Training updated to make staff aware of this scam. Staff to not allow any code to be presented.	
	10	Bring your own devices' (BYODs)		Customers using own device to use wallets on their devices to pay. Risk of customers betting through credit cards through a 'wallet' solution.	Elavon our payment processer currently blocks all wallet payments as it identifies all wallet payments as credit cards even if it is a debit card on the wallet.	

Area		Risk	RAG Status	Definition	Risk Controls	RAG Status Post Control
Customer Risk	1	Anonymity		Customers that are predominately cash-based may convert criminal funds into legitimate funds.	Many customer enjoy using cash to budget their gambling so prevention of this can damage customer's	

					ability to gamble within their limits. Customers are monitored with Nom Du Plumes with their trading history so that further investigation can take place if needed. operates a strict 'Permission to Lay' (PTL) policy in respect of bet acceptance. This process also involves an assessment from shop and trading staff from a POCA and AML perspective before authorising a bet to be accepted.	
	2	Customer Appearance/ Lifestyle Inconsistent With Spend		Customers who bet with funds that are known to be outside of their means, lifestyle, or profile (i.e. unemployed, age, known job does not tally with time spent in shop).	Customers are monitored with Nom Du Plumes (or actual names if known) with their trading history so that further investigation can take place if needed should financial thresholds set by the compliance team be met.	
	3	Receipts For Winning Bets		Customers requesting receipts do so in an attempt to gain 'evidence' of legitimate origins of criminal funds. Also risk of trying to use other customer receipts as well as own.	Jenningsbet operate a strict no receipts policy for betting transactions. Any request would have to be made directly to the Compliance team.	
	4	Runners/ OGCs		A runner is a customer acting on behalf of another individual but not disclosing this. Risk of said individual attempting to disassociate themselves with their funds that could be proceeds of crime.	All bets are monitored and patterns and trends identified on bets within a localised area by Race Room.	
Customer Risk	5	Customer Using Multiple Jenningsbet Branches		Customer using multiple locations using criminal funds to avoid detection by becoming more difficult to monitor. The Gambling Commission has seen an increase of this risk with OGCs.	All bets are monitored and patterns and trends identified on bets within a localised area by Race Room. Strong communication protocols in place between Race Room and shops.	
	6	Customer Using Multiple Branches Including Other Operators		Customer using multiple locations using criminal funds to avoid detection by becoming more difficult to monitor.	All bets are monitored and patterns and trends identified on bets within a localised area by Race Room. Strong communication protocols in	

					place between Race Room and shops. Shared intelligence working groups both on a local level through BetWatch groups and on a larger scale with trade association and police.	
	7	Significant Changes In Betting Patterns and Behaviour		Customer displays irregular activity, for example betting or gaming level increases dramatically, with no indication of the source of funds.	All bets are monitored and patterns and trends identified on bets within a localised area by Race Room. Strong communication protocols in place between Race Room and shops.	
	8	High-Value Staking Customers		Significantly higher level of spend than the average customer in the locality may indicate an increased risk of criminal funds being used.	Customers are monitored with Nom Du Plumes (or actual names if known) with their trading history so that further investigation can take place if needed should financial thresholds set by the compliance team be met.	

Area		Risk	RAG Status	Definition	Risk Controls	RAG Status Post Control
Employee Risk	1	Collusion		Employees working with friends or customers to manipulate trading to conceal criminal suspicious activity	Security team monitor live bets and employee till transactions to identify unusual or suspicious activity from employees. operates a strict 'Permission to Lay' (PTL) policy in respect of bet acceptance. This process also involves an assessment from shop and trading staff from a POCA and AML perspective before authorising a bet to be accepted.	
	2	Suspicious Activity Missed or Not Acted Upon		Employees either missing or not acting upon suspicious alerts being raised through the gaming machines when customers display unusual activity that may be ML.	Customers are unable to play on a gaming machine once suspicious activity alert is raised without employee manual reset.	
	3	Non-Compliance		Employees may deliberately avoid	All bets are monitored and patterns and trends	

		with AML/CTF Controls		following controls either due to commercial considerations such as increased shop performance or unwillingness to increase workload	identified on bets within a localised area by Race Room. Till system means concealing shop activity is not possible.	

Area		Risk	RAG Status	Definition	Risk Controls	RAG Status Post Control
Product Risk	1	Payment Following Minimal Or No Play on Gaming Machines		Customer may attempt to launder funds by uploading money onto a gaming machine and printing a receipt for collection at the counter having spent a minimal amount or no spend	Gaming Machines will cause a suspicious activity alert if a customer attempts to withdraw £300 or more in a single action without playing through at least 75% of the funds. When used in conjunction with CCTV, can be used to identify customers suspected of money laundering and offer law enforcement an audit trail. Gaming machine manufacturers must comply with the gaming machine technical standards (GMTS), which provide some protection against money laundering vulnerabilities	
	2	Payment Following Minimal Or No Play on Gaming Machines SSBTs		Customer may attempt to launder funds by uploading money onto a gaming machine and printing a receipt for collection at the counter having spent a minimal amount or no spend	Automatic alerts and/or triggers for example, redemption and churn level limits. More collaboration is needed in this area on an industry level with the suppliers and this is an area of focus with the BGC.	
	3	Gaming Machine Play		Gaming Machines used as a facility for large spending of funds that are proceeds of crime	Regulations imposing controls on B2 gaming machines to limit spins over statutory monetary limits has decreased the amount a customer can play in a short time undetected by staff	
		Low risk wagering/ covering all		Customer may bet on a combination of 'non-runners', short priced	All bets are monitored and patterns and trends identified on bets within a	

		outcomes/ cash out (OTC)		favourites, attempting to place late bets and/or betting on all selections on an event in order to either 'guarantee' or improve their chances of a return to launder criminal funds	localised area by Race Room.	
		Low risk wagering/ covering all outcomes/ cash out (SSBT)		Customer may bet on a combination of 'non-runners', short priced favourites, attempting to place late bets and/or betting on all selections on an event in order to either 'guarantee' or improve their chances of a return to launder criminal funds	Automatic alerts and/or triggers for example, redemption and churn level limits. Value only tickets cannot be paid out in shops that they were not created to ensure customers cannot disguise how the tickets value was created.	

Area		Risk	RAG Status	Definition	Risk Controls	RAG Status Post Control
Other Risk	1	Third-party suppliers		Third-party suppliers carry risk of financial crime that could impact Jenningsbet	Relevant third-parties are regulated, and therefore scrutinised independently in relation to AML/CTF. There is no requirement for Jenningsbet to undertake further due diligence.	

Training

It should be noted that our employee training forms as a primary control against the majority of the aforementioned risks. Staff are trained on the regulatory framework Jennings operates in with emphasis on their individual responsibilities and accountability. Further detail of each control is found in our AML Policy and Procedures and Controls.