KPMG

THOMSON REUTERS®

GAMLG's AML Risk Assessment for Licensed Betting Offices (LBOs) and Remote Gambling Industries

GAMLG

GAMBLING ANTI-MONEY LAUNDERING GROUP

TABLE OF CONTENTS

Keith Bristow

FROM THE CHAIRMAN

It gives me great pleasure to introduce our first publication of the national GAMLG Money Laundering Risk Assessment, for the remote and Licenced Betting Office (LBO) sectors.

In January 2016, I was delighted to accept the position of Chairman, to the Gambling Anti-money Laundering Group (GAMLG) which had been recently formed by the Remote Gambling Association (RGA) and the Association of British Bookmakers (ABB). The sectors represented, account for over 70% of the British gambling market.

The remit of the Group is to produce industry Codes, promulgate best practice, provide advice to the industry and liaise and negotiate with other key stakeholders. Where appropriate, GAMLG will act as a conduit for industry views to be put forward to national and international authorities on any money laundering issues that are of relevance to it. At the discretion of its membership, it can also involve itself in other areas such as improved information-sharing arrangements between operators, including trends, emerging threats, and where possible, data.

We should never forget that serious and organised criminals commit crime to make money, causing untold misery in the process. The total amount of money laundered into and through the UK is unknown, but we do know that it will include the proceeds of virtually all serious and organised crime in the UK as well as significant sums from overseas. Criminals use a range of dishonest methods to launder their criminal profits, including gambling, which can provide a credible explanation for a source of wealth.

I have been impressed by the commitment of the gambling industry to tackle money laundering. The industry acknowledges that there is more to be done. As Chair of the GAMLG, I work constructively with the industry to continue to drive up standards and, when necessary, robustly challenge current policy and practice. By making it even more difficult for criminals to exploit the gambling industry, we will make a real contribution to the protection of UK businesses and communities.

As a foundation for our key projects, we have produced this GAMLG Risk Assessment for the Licensed Betting Office and Remote Gaming sectors. In this brochure, we define the areas that we have identified as risk areas for money laundering, the level of risk they represent and the residual risk that remains following the controls that must be in place. The detail behind the risk tables in this brochure is both considerable and robust and is shared between 47 compliance professionals from 22 operators.

The identification of these risks and the industry guidance that will follow will forge best practice to effectively minimise the risk of money-laundering, in the gambling sectors that we represent.

Keith Bristow QPM
Chairman
Gambling Anti-Money Laundering Group

INTRODUCTION

This is the first risk compilation of the money laundering and terrorist financing (ML/TF) risks within the gambling sector, prepared by the GAMLG. The assessment has been undertaken in-line with the 3rd AML Directive and has been established, following consultations and interaction with both remote (online) and LBO operators.

Although the HM Treasury UK's National Risk Assessment has assessed the gambling sector as low risk, a number of vulnerabilities within the sector were highlighted. These, in addition to other vulnerabilities within the remote and LBO sectors, recognised by the GAMLG group as being at risk of abuse or exploitation by criminals, are addressed in this document.

This sector risk assessment intends to highlight such areas; its key objectives are as follows:

- Identify specific risks posed to operators within the gambling sector.
- Promote better understanding of threats and risks within the sector.
- Provide guidance to operators on the specific vulnerabilities of the sector as well as the mitigation controls available to combat ML/TF risks.
- Encourage operators to examine their own ML/TF risks in light of the sector risk assessment.

An awareness at sector level of the threats, vulnerabilities and consequences posed by ML/TF is vital to the integrity of the gambling sector and how it is perceived by the public, as well as other sectors, whether regulated or not.

SCOPE

It is important to note that the risks captured within this document by the GAMLG are based on the nature of the business undertaken by the majority of the industry. This document is not intended to replace operator-specific risk assessments and it remains the responsibility of each operator to carefully examine its products, customers, geographical reach and operational setup to identify, understand, assess and put in place proportionate control measures, suitable to its specific risks.

Control measures within the assessment are the agreed industry standard; the strength of these controls will differ from operator to operator dependant, amongst other factors, on how vigorous the risk appetite of the operator is. Some operators may allocate additional resources to control certain risks, or may in fact have taken the decision to wholesale de-risk the area; such decisions can only be made at operator level.

Only risks which are within operators' control are included in this document. For example, although the risk of criminals setting up or controlling a gambling operator is a significant one, such a risk can only be mitigated at supervisory level by subjecting potential licensees through a 'fit and proper' test to ensure that criminals are prevented from being professionally accredited.

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 of problem gambling (or both). It is plausible that an individual attempting to spend criminal proceeds or launder money could also be a problem gambler, but one does not necessarily follow the other. Responsibility lies with the operator to understand these dynamics and to mitigate any risks to the licensing objectives. Although it is accepted by operators that the areas of anti-money laundering and responsible gambling are intrinsically interlinked, it should be noted that any risks associated with problem gambling are not within the scope of this risk assessment, which focuses explicitly on the areas of ML/TF.

Remote and LBO risks are shown in this document separately. Land-based casinos, arcades (inland, seaside or service station) and bingo clubs are out of scope.

METHODOLOGY

In identifying potential risks and threats across the industry, the following categories have been considered:

- **Customer risk** – specific categories of customers and the resulting business relationships.
- **Payment risk** – payment methods offered by operators and the degree to which their specific characteristics are vulnerable to ML/TF threats.
- **Geographical risk** – the risks posed by geographical factors (remote only).
- **Product risk** – products offered and the degree to which their specific characteristics may be attractive for the purpose of money laundering or financing terrorism.
- **Employee risk** – the risks posed by the employees of every operator.

Each category will pose varying degrees of risk which will vary from one operator to another.

A small number of the risks can also be described as red flags, but are none the less included as they are directly relevant to the assessment and better enable operators to mitigate the risks.

This document reflects potential ML/TF risks which have been analysed to assess the probability of them occurring and the potential impact they may have on an operator, should they occur.

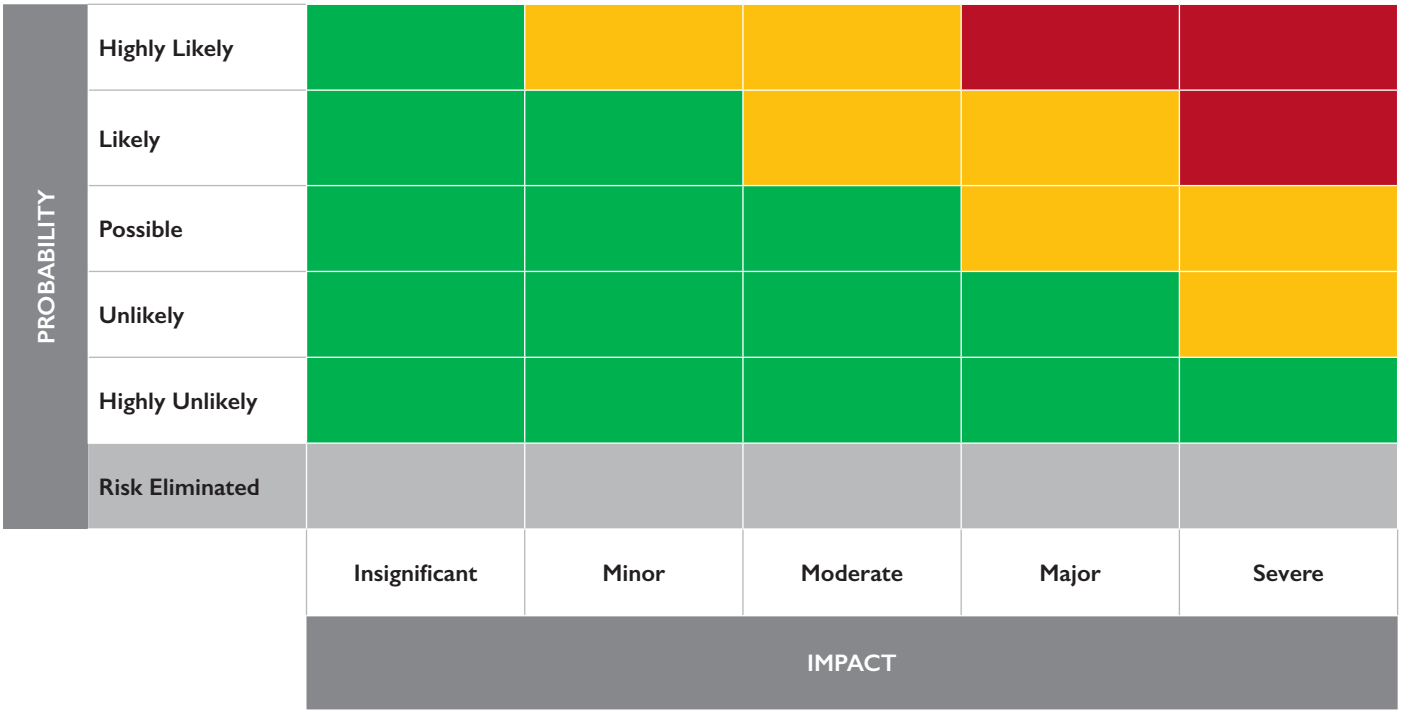
A comprehensive assessment of all risks was undertaken by GAMLG members and industry external experts, based on the relationship between the risk probability and the risk impact. The full Risk Assessment document was then shared with the Gambling Commission for final scrutiny. The tables included in this document reflect the initial risk assessment level and the residual risk level after the controls are deployed.

Risk probability is the chance of an identified ML/TF risk materialising as part of everyday operations across the industry. This can also be interpreted as the vulnerability of each area identified and how likely the area is to be exploited by criminals. Some risks are therefore more likely to occur than others.

Risk impact describes the expected damage to the operator and industry should the identified ML/TF materialise without any specific control measures in place. The potential impact is not the same for all identified risks as some may have a greater impact than others. When determining the impact of an identified risk, consideration has been given to factors such as:

- Facilitation of criminal conduct
- Risk of regulatory fines and legal prosecution
- Reputational damage to operators and/or the industry overall
- Loss of business as a result of customer rejection

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. This will determine the correct proportionality for the control measures, which need to be put in place. This is sometimes referred to as the 'inherent risk' – the risk that resides in the essential nature of a product, feature, payment method characteristic etc., which must be addressed to avoid that risk materialising; and/or to mitigate the effect of that materialisation. The table below demonstrates how GAMLG arrived at our risk assessment and the red/amber/green determination.



Control measures are applied to each identified risk, to bring the risk within an acceptable level; what is 'acceptable' differs from operator to operator. A residual risk assessment of red/amber/green is calculated by combining the probability of the risk materialising and the resulting impact or damage after control measures have been applied. What remains, the residual risk, is the accepted level of risk after application of AML/CTF controls. The residual risk categories are monitored and re-assessed, where there is a change in the original risk evaluation.

The risk level assigned to each identified risk, has been compiled and reviewed by a number of industry experts based on knowledge, experience and evidence from within their own businesses.

The control measures' effectiveness in the industry is dependent on the individual operator's rigorous and diligent application of them. Effective governance arrangements and oversight is essential in this process, and individual companies must ensure that senior management is fully engaged in the process.

Additionally, the evaluation of an operator's individual risk assessment will be dependent upon the specifics of each business and the mitigation measures applied. Whilst the inherent risk scores are likely to be similar across the industry, residual risk scores can be expected to differ dependent upon an operator's mitigation measures and risk appetite.

Risk assessments should be reviewed and refreshed on an annual basis and in the event of material changes to the risk environment. This ensures that new risks are effectively assessed and the appropriate control measures are put in place for emergent technologies, such as virtual currencies (which are not currently prevalent in the industry). In addition, the ongoing evaluation of existing risks in relation to the current risk environment is also reviewed.

The two sectors, (Remote and LBOs) are separated in this document into two sets of tables and detail the **risk** and **definition** for 24 remote and 20 LBO retail risks, in up to five risk areas (Customer, Payment, Product, Employee and Geographical (remote only). The **GAMLG AML Risk Assessment** and **Residual Risk Assessment after Controls** columns are simplified to show, by coloured symbols, the original level of risk and the residual risk when the controls are applied.

This Risk Assessment will determine the focus and next steps for GAMLG in order to promote guidelines and best practice across the LBO and remote sectors, for varying sizes and types of operators within our membership.

LICENSED BETTING OFFICES – RISKS

AREA		RISK	DEFINITION	GAMLG AML RISK ASSESSMENT	RESIDUAL RISK ASSESSMENT AFTER CONTROLS
CUSTOMER RISK	1	Anonymity	Unlike the online sector (where the customer is known to the operator from registration), betting shops are predominantly cash-based and therefore afford a level of anonymity to the customer. This anonymity brings with it the risk that LBOs could be abused as a vehicle through which criminals look to 'wash' funds or spend the proceeds of crime.		
	2	Customer appearance inconsistent with customer spend	There is a risk that the funds a customer spends represent the proceeds of crime which the customer intends to launder through, or spend with, the operator. A potential red flag indicating such a risk is customers apparently spending beyond their means. This may specifically manifest itself in a marked difference between customer lifestyle and/or appearance and the amount of money spent with the operator.		
	3	Receipts for winning bets	There is a risk that customers requesting receipts of winnings bets (either over the counter or from machines) do so in an attempt to gain what appears to be evidence of the legitimate origins of criminal funds. Although there may be a perfectly good reason behind such requests, this is not considered 'normal' behaviour for a recreational gambler. A heightened risk exists where individuals are requesting receipts for winning bets from other customers in the shop, or looking for such receipts in waste bins.		
	4	Runners	The term 'runner' describes an individual who is suspected of acting on behalf of a third party but does not disclose that information. There is a risk that a runner may be used by an individual who is looking to disassociate himself from criminally derived property by creating distance from the funds. This in turn means that the true beneficial owner of the funds is not known.		
	5	Requests to pay out winnings via different payment method	An area of risk is a customer looking to have winnings returned via a different payment method to that used to place the bet or initially gamble with. This may be where cash is used to pay for a bet/game and winnings are requested to be paid via debit card or cheque, or vice versa.		
	6	Customer using multiple premises – same operator	There is a risk that criminals target betting shops in order to legitimise large quantities of cash derived from criminal activity. To this end, a customer may use multiple shops of the same operator in an attempt to reduce the possibility of his business being flagged for monitoring or to avoid cumulative spend being derived correctly.		
	7	Customer using multiple premises – different operators	Customers are free to spread their activities across a variety of operators, and each operator may therefore have little in terms of customer contact from which to identify unusual behaviour. There is a risk that criminals target betting shops in order to legitimise large quantities of cash derived from criminal activity. To this end, a customer may use multiple shops of different operators in an attempt to reduce the possibility of his business being flagged for monitoring or to avoid cumulative spend being derived correctly.		
	8	Drastic changes/ significant increase in betting behaviour	A drastic change in betting behaviour (i.e. unusually high activity when comparing to what may reasonably be deemed normal expected activity from the customer in question) may indicate that the individual is looking to abuse the operator for money laundering purposes.		
	9	High-value staking customers	Where a high-value stake is made in a single transaction or cumulative stakes of significant value are placed, an increased risk of ML/TF activity is posed – the stake or stakes may represent the proceeds of crime which the customer intends to launder through, or spend with, the operator.		
	10	Use of LBOs to withdraw online funds	Operators who accept business both online and in LBOs may be at risk of having such a setup abused by customers looking to withdraw funds held in online accounts in cash in an attempt to bypass payment method rules and controls.		

LICENSED BETTING OFFICES – RISKS

AREA		RISK	DEFINITION	GAMLG AML RISK ASSESSMENT	RESIDUAL RISK ASSESSMENT AFTER CONTROLS
PAYMENT RISK	1	Dye-stained banknotes	There is a risk that criminals target betting shops in an attempt to launder bank notes which have been permanently stained as a result of coming into contact with cash degradation dye released during attempted cash robberies. Criminals may insert stained notes into gaming machines and then seek to obtain clean notes following the printing of receipts for collection at the counter.		
	2	Use of cash	There is a risk that criminals in possession of cash representing the proceeds of crime may target betting shops in order to convert the criminal funds into legitimate funds. Cash has a number of characteristics open to abuse by criminals including its anonymity and difficulty to trace; therefore customers using cash pose a higher ML/TF risk to operators.		

LICENSED BETTING OFFICES – RISKS

AREA		RISK	DEFINITION	GAMLG AML RISK ASSESSMENT	RESIDUAL RISK ASSESSMENT AFTER CONTROLS
PRODUCT RISK	1	Payment following minimal or no play (gaming machines)	'There is a risk that a customer may attempt to launder funds through a gaming machine, by funding the machine either through cash or debit card and then printing out receipts for collection at the counter, following minimal or no play.		
	2	Payment following minimal or no play (SSBTs)	'There is a risk that a customer may attempt to launder funds through an SSBT, by funding the machine either through cash or debit card and then printing out receipts for collection at the counter, following minimal or no play.		
	3	Low risk wagering/ covering all outcomes/ cash out (OTC)	There is a risk that a customer may place bets OTC at short odds either with large stakes or high frequency/low stakes, cover all outcomes of an event or partake in non-recreational cash out activity in order to wash through criminal funds or to make returned funds appear as legitimate.		
	4	Low risk wagering/ covering all outcomes/cash out (SSBTs)	There is a risk that a customer may place bets using SSBTs at short odds either with large stakes or high frequency/low stakes, cover all outcomes of an event or partake in non-recreational cash out activity in order to wash through criminal funds or to make returned funds appear as legitimate.		

LICENSED BETTING OFFICES – RISKS

AREA		RISK	DEFINITION	GAMLG AML RISK ASSESSMENT	RESIDUAL RISK ASSESSMENT AFTER CONTROLS
EMPLOYEE RISK	1	Employees	Employees may attempt to carry out acts of collusion or record manipulation in order to facilitate ML/TF activity. It is possible that employees who live and work in the same local community would be at risk of helping friends or associates to launder criminal funds and accepting cash bribes/incentives for doing so.		
	2	Non-compliance with AML/CTF controls due to commercial considerations	Employees may pose a risk by allowing commercial considerations to override AML/CTF compliance in shops where a significant level of the business depends on one or two customers, resulting in reluctance to escalate any potential concerns to the AML team/MLRO.		
	3	Staff knowledge	Employees may pose a significant risk where they have either not received adequate training to enable them to identify potential ML/TF issues, or where they are unable to highlight such issues through the established channels.		

LICENSED BETTING OFFICES – RISKS

AREA		RISK	DEFINITION	GAMLG AML RISK ASSESSMENT	RESIDUAL RISK ASSESSMENT AFTER CONTROLS
UNUSUAL ACTIVITY	1	Unusual activity	There is a risk that instances of unusual activity are not escalated by employees where there is an indication that a customer and/or employee may be involved in potential ML/TF activity. This is applicable to the Customer, Payment, Product and Employee risk areas.		

REMOTE OPERATORS – RISKS

AREA		RISK	DEFINITION	GAMLG AML RISK ASSESSMENT	RESIDUAL RISK ASSESSMENT AFTER CONTROLS
CUSTOMER RISK	1	Unverified or front accounts	There is a risk that an account may be opened using false information or by someone other than the registered individual for the purpose of carrying out ML/TF activity. An unverified or front account poses a risk as the operator does not know with whom it is transacting.		
	2	High-value depositing customers	Where a high value deposit is made in a single transaction or cumulative deposits of significant value are made over a short time frame, an increased risk of ML/TF activity is posed – the deposit or deposits may represent the proceeds of crime which the customer intends to launder through, or spend with, the operator.		
	3	Politically Exposed Persons (PEPs)	There is a higher-risk associated with individuals who have a high political profile or have held public office (past or present), as their positions may make them vulnerable to corruption and bribery therefore increasing the risk of accounts being funded by the proceeds of crime by such individuals.		
	4	Prohibited relationships and transactions (sanctions)	There is a risk that an individual subject to sanctions may attempt to open an account and transact with an online operator. It is a criminal offence to transact with individuals who are subject to certain types of sanctions such as asset freezes.		
	5	Dormant accounts	There is a risk that a customer may deposit funds and then not use his account for a significant period of time before looking to withdraw the funds at a later stage, following very little or no activity, in the hope to distance himself from his crimes by the passing of time.		
	6	Source of funds/wealth is unknown for higher-spending customers	If higher-spending customers are allowed to play without source of funds/wealth being established on a risk-sensitive basis, an increased risk of ML/TF activity is posed.		
	7	Change to registered personal details for account holders	A customer who changes his personal details such as residential address, email address or telephone number poses an increased ML/TF risk as he may not provide his up-to-date information to an operator. This poses a particular risk where the outdated information is used as part of ongoing monitoring (for example compromising sanctions screening processes) or enhanced due diligence checks and investigations.		
	8	Drastic changes in betting behaviour	A drastic change in betting behaviour (i.e. unusually high activity when comparing to what may reasonably be deemed normal expected activity from the customer in question) may indicate that the account is now being used, by the customer or by someone on whose behalf the customer is acting, for money laundering purposes.		
	9	Multiple payment methods	Individuals using multiple payment methods to fund their accounts without obvious rationale behind such behaviour (e.g. registration of a new credit/debit card to replace an expired one) may be attempting to structure deposits representing the proceeds of crime in order to avoid detection. The use of multiple methods enables an individual to move funds easily to other betting sites or bank accounts. This may include both refundable and non-refundable payment methods.		

Risk Operators – Risks
Customer Risk *continued*

REMOTE OPERATORS – RISKS

AREA		RISK	DEFINITION	GAMLG AML RISK ASSESSMENT	RESIDUAL RISK ASSESSMENT AFTER CONTROLS
CUSTOMER RISK *continued*	10	Payment card ownership	Where funds are deposited from a card which does not belong to the customer or is a corporate card, there is an increased risk that the customer may be using the card to either deposit unauthorised funds or criminally obtained funds. With corporate cards, there is a risk that a business is being used as a front for criminal activity, therefore corporate cards could be issued to disguise or transfer the proceeds of crime.		
	11	Multiple accounts - same operator	There is a risk that a customer may open multiple accounts using different names and identities, making it difficult to verify the real account holder (beneficial owner) and/or the source of the funds.		
	12	Multiple accounts - different operator	Customers are free to spread their activities across a variety of operators, and each operator may therefore have little in terms of transaction history from which to identify unusual behaviour. This may also result in customer activity levels with single operators falling below internal reporting thresholds in accordance with the risk-based approach, where the customer would therefore not be highlighted for further investigation despite significant levels of deposit or drop activity with all operators.		
	13	VIP enhancements	There is a risk that VIPs are upgraded onto loyalty/reward schemes without having undergone proper due diligence, therefore potentially rewarding customers who have deposited the proceeds of crime with the operator. Additionally, considering the higher monetary values involved in such relationships, should any operator AML/CTF failings be published, they are likely to attract significant national press interest, negatively impacting on public perception of the integrity of the gambling sector.		
	14	Customer-to-customer fund transfers	There is a risk that customers could pass the proceeds of crime from one account to another account held with the same operator (belonging to a different individual) in order to create distance and confuse the money trail or transfer funds as a way of paying for goods or services related to criminal activity.		

REMOTE OPERATORS – RISKS

AREA		RISK	DEFINITION	GAMLG AML RISK ASSESSMENT	RESIDUAL RISK ASSESSMENT AFTER CONTROLS
PAYMENT RISK	1	Cash-based payment methods	Customers using cash-based payment methods pose a higher ML/TF risk to operators as the source of funds is in the main unknown and difficult to trace. This type of payment method is often also non-refundable, meaning that withdrawals must be processed via an alternative source. Also included in this risk (for operators who have both an online and retail betting presence) is the use of LBOs to fund an online account using cash. There is a risk that customers may abuse these characteristics in order to carry out ML/TF activity through their betting accounts.		
	2	eWallet payment methods	eWallets payment methods are potentially higher-risk payment methods as a potential means to mask the true origins of the funds deposited with the operator. The use of eWallet payment methods enables an individual to move funds easily to other betting sites, bank accounts or spend via associated debit/credit cards. A customer depositing via an eWallet may pose an increased ML/TF risk to operators as the source of funds is difficult to trace and this payment method type offers a relative level of anonymity to the customer.		

REMOTE OPERATORS – RISKS

AREA		RISK	DEFINITION	GAMLG AML RISK ASSESSMENT	RESIDUAL RISK ASSESSMENT AFTER CONTROLS
PRODUCT RISK	1	Withdrawing without play/ low-risk wagering/ covering all outcomes/ cash out	There is a risk that a customer may deposit criminal funds into his account and then withdraw them without wagering in any product, following minimal play, low-risk wagering activity, by covering all outcomes or by using the cash out facility.		
	2	Poker product: Peer-to-peer gambling	Poker is classed as a higher-risk product for ML/TF purposes due to the potential for collusion and soft play as there is a risk for money to be deliberately passed between players on the same network which could be the proceeds of crime or funds could be passed to pay for goods or services related to criminal activity.		

REMOTE OPERATORS – RISKS

AREA		RISK	DEFINITION	GAMLG AML RISK ASSESSMENT	RESIDUAL RISK ASSESSMENT AFTER CONTROLS
EMPLOYEE RISK	1	Employees	Employees potentially pose a significant ML/TF threat by means of collusion through play, product or record manipulation. Without appropriate identification processes in place, operators may become vulnerable.		
	2	Staff knowledge	Employees may pose a significant risk where they have either not received adequate training to enable them to identify potential ML/TF issues, or where they are unable to highlight such issues through the established channels. Without sufficient training and standards in place, there is a risk that staff may become involved in assisting in the commission of an ML offence.		

REMOTE OPERATORS – RISKS

AREA		RISK	DEFINITION	GAMLG AML RISK ASSESSMENT	RESIDUAL RISK ASSESSMENT AFTER CONTROLS
GEOGRAPHICAL RISK	1	Activity from outside a customer's registered country	A customer logging into his account from outside of his registered country poses a potential risk to an operator as the customer may not be who he claims to be and the information used to verify the account as well as the source of funds may be incorrect as a result. This can pose an increased level of risk where logins are made from high-risk countries.		
	2	Mismatch in country of residence/card country/bank country	There is a risk that a customer may be attempting to send funds to a source outside of his residential country in order to disguise the origin and/or the destination of the funds. This can pose an increased level of risk where payments come from high-risk countries.		
	3	Accepting business from high-risk jurisdictions	There is a risk that customers from countries which have been highlighted by sources such as FATF as having strategic AML/CTF deficiencies look to abuse the sector for ML/TF activity. There is also a risk when accepting customer from countries that have high levels of corruption as this increases the risk of ML taking place.		

REMOTE OPERATORS – RISKS

AREA		RISK	DEFINITION	GAMLG AML RISK ASSESSMENT	RESIDUAL RISK ASSESSMENT AFTER CONTROLS
UNUSUAL ACTIVITY	1	Unusual activity	There is a risk that instances of unusual activity are not escalated by employees where there is an indication that a customer and/or employee may be involved in potential ML/TF activity. This is applicable to the Customer, Payment, Product, Employee and Geographical risk areas.		

For more information about
GAMLG's Risk Assessments please visit
www.gamlg.org

GAMLG

GAMBLING ANTI-MONEY LAUNDERING GROUP