

**Chongie Entertainment UK Limited**

The logo for Little Vegas is centered on a dark red rectangular background with rounded corners. The background has a subtle, repeating diamond or quilted pattern. The words "LITTLE VEGAS" are written in a bold, yellow, sans-serif font. Below the text is a horizontal line of small yellow dots.

**LITTLE VEGAS**

**Proceeds of Crime and  
Anti Money Laundering  
Policy**

- 1 POLICY PURPOSE**
- 2 PROCEEDS OF CRIME (POC) & MONEY LAUNDERING (ML)**
- 3 POCA OFFENCES & PENALTIES**
- 4 KNOWLEDGE OR SUSPICION**
- 5 RESPONSIBILITIES**
- 6 PRODUCTS & RISK MITIGATION**
- 7 RISK TRIGGERS**
- 8 CUSTOMER MONITORING**
- 9 SYSTEM CONTROLS**
- 10 PROACTIVE ANALYSIS- THRESHOLD REVIEW & REPORTS**
- 11 SUSPICIOUS ACTIVITY REPORTS (SARs)**
- 12 SAR MONITORING AND TERMINATION OF CUSTOMER RELATIONSHIPS**
- 13 PREJUDICING AN INVESTIGATION**
- 14 ADVERSE INFORMATION & POLICE INVOLVEMENT**
- 15 INTERNAL RISKS**
- 16 TRAINING AND SCREENING**
- 17 MONITORING THE POLICY**

## **1 POLICY PURPOSE**

The purpose of this document is to detail the responsibilities of the Company and its staff in relation to the Proceeds of Crime Act 2002 (POCA), Terrorism Act 2000 and to uphold the licensing objective of 'Preventing gambling from being a source of crime or disorder, being associated with crime or disorder or being used to support crime' as outlined within the Gambling Act 2005.

In addition, the contents of the document will outline our Company's policies and procedures to prevent the Company being used in connection with money laundering or terrorist financing as well as our continued compliance with anti-money laundering, counter terrorist financing, licensing and legislative requirements.

Chongie Entertainment UK Limited is committed to ensuring that all necessary safeguards are in place in regard to the receipt of money in order to avoid it being used to launder money that may originate from the proceeds of crime.

This document is based on the guidance issued by the Gambling Commission from time to time, as well as the findings of the Money Laundering and Terrorist Financing Risk Assessment (LCCP 12.1.1)

## **2 PROCEEDS OF CRIME & MONEY LAUNDERING**

### *2.1 Proceeds of Crime*

The Proceeds of Crime can be broadly defined as property from which a person benefits directly or indirectly, by being party to criminal activity -e.g. stolen money, money from drug dealing, tax evasion or stolen 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.

### *2.2 Money Laundering*

Money Laundering is a term used to describe the practice of converting money that has been unlawfully or criminally obtained into legitimate funds, concealing and disguising the original source of the funds.

### *2.3 Differences*

The law does not make any distinction between these two activities. The action we should take, and the penalties for not taking action are the same for both.

Staff will be trained according to their seniority and role in the business.

## **3 PROCEEDS OF CRIME ACT (POCA) OFFENCES & PENALTIES**

There are 3 key offences under the POCA that are applicable to anyone who knows or suspects that property relates to the Proceeds of Crime:

- Section 327 states that a person commits an offence if they conceal, disguise, convert, or transfer criminal property in the UK.
- 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.

- Section 329 states that a person commits an offence if he or she acquires, uses, or has possession of criminal property.

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.

There is a defence available for a person to show that they made an authorised disclosure under sections 338 and 339, either for an employee to report to the Nominated Officer (Dobromir Baltadzhiev), and further for responsible parties in senior management to assess and report where they believe knowledge or suspicion exists to the National Crime Agency (NCA).

Once a report has been made, the Nominated Officer (Dobromir Baltadzhiev) will consider whether they hold knowledge or suspicion based on the information provided. However, responsible parties in senior management may commit an offence under section 332 if there is a failure to report knowledge or suspicion to the NCA as soon as reasonably practicable after the information has been received. The sanction under POCA is a prison term up to 5 years, a fine, or both.

It is also an offence under section 342 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.

#### **4 KNOWLEDGE OR SUSPICION**

Chongie Entertainment UK Limited and its employees have an obligation to report when we either have knowledge or suspicion that another person is using the POC or engaged in ML.

The POCA regulations do not define knowledge or suspicion, but case law has provided guidance.

Common sense provides that if, for example, a customer confirms they are laundering money or using money from a robbery, the member of staff would in fact know rather than suspect. Courts have previously gone further and also defined knowledge to include situations where the facts would be clear to an honest and reasonable person. It could also include a member of staff turning a blind eye, for example, if staff do not make normal enquiries of a customer where they believe they already know the answer and do not want to hear it.

Suspicion is subjective and may be based on picking up something unusual or where facts do not tally up. Suspicion does not need to be based on actual facts, but there needs to be some satisfaction beyond speculation that the customer is involved in the use of the POC or ML. A feeling of unease does not amount to suspicion.

#### **5 RESPONSIBILITIES**

The POCA and AML regime within Chongie Entertainment UK Limited is managed by the Nominated Officer (Dobromir Baltadzhiev) and supported by senior management.

All staff have a role to play in combatting the use of criminal proceeds and ML, and are trained to pick up triggers which may lead to concern and further suspicion or knowledge.

Staff are also trained to report general concerns or otherwise knowledge or suspicion to the Nominated Officer (Dobromir Baltadzhiev). Where knowledge or suspicion of money laundering is believed to exist, the Nominated Officer (Dobromir Baltadzhiev) will determine whether a Suspicious Activity Report (SAR) should be raised with the NCA.

## **6 PRODUCTS & RISK MITIGATION**

Chongie Entertainment UK Limited runs Adult Gaming Centre facilities in the UK.

To identify and manage the risks associated with the above products, Chongie Entertainment UK Limited applies controls in four broad ways.

*RISK TRIGGERS:* Training key staff to be aware of risk triggers which may be indicative of ML or the use of POC and how to report concerns.

*CUSTOMER MONITORING:* Providing facilities to allow Chongie Entertainment UK Limited to monitor customers, allowing staff to log consumer information, transactions and emerging concerns. These records are kept in the tablets on site and in the cloud.

*SYSTEM CONTROLS:* Implementing controls to mitigate areas of potential risk and highlight potential irregularities.

*PROACTIVE ANALYSIS:* Carrying out proactive analysis of purchasing activity to help detect unusual activity and risk triggers. This is supported by record keeping, monitoring and customer reviews.

Each is considered in turn below. This policy is supplemented by the Customer Due Diligence and “Know Your Customer” Procedures set out below and in the Compliance Pack and the Customer Interaction Policy.

## **7 RISK TRIGGERS**

Considering the above product type, there are different types of activity or customer behaviours which could lead to cause for concern leading to the possible formulation of knowledge or suspicion that an individual is participating in gambling activity with the POC or involved in ML.

Some examples of risk triggers are:

- Geographical Risk - a customer being located in a high risk jurisdiction. A high risk jurisdiction includes those on the FATF Black List and the FATF Grey list, both of which can be accessed online by the MLRO
- A customer behaving in a secretive manner, refusing to speak to staff or concealing funds
- Customers appearing to engage in potential criminal activity, or discussing potential criminal activity
- Customers appearing to have a sudden change in financial circumstances without a reasonable explanation

- Staff knowledge or reasonable suspicion of local crime, or individuals engaged in local crime
- Asking to or attempting to lend money between customers, staff with a reasonable knowledge or suspicion of money lending taking place
- Attempting to cash out another customer's ticket
- Customers playing with a large volume of coins, or attempting to exchange a large volume of coin for notes
- Attempting to scan a gaming machine by using a "note fishing technique" (by attaching a small rope to the note to fool the machine into registering it, despite the note being pulled back out of the machine). This could be identified by frequent large wins on category C machines
- Machine play which indicates a possible involvement in POC or ML include:
  - Loading credit and trying to cash the ticket after little or no play.
  - Trying to use cash to load credit and asking for cheque or debit card payment (not possible on the CEL system).
  - Asking or attempting to use one debit card to load credit and then using another to collect winnings (not possible on the CEL systems)
  - Requesting receipts/copies of their tickets from their pay outs.

These behaviours may be identified by any employee, and are most likely to be recognised by staff working in the Adult Gaming Centres. Full training is carried out on induction and at 6 monthly refreshers. All staff are therefore fully equipped with the skills they need to identify any suspicious behaviour.

Staff are encouraged to ask themselves the following questions to help them understand the nature of the situation. In some circumstances these may be more appropriate for EDD conducted by management (Please see below) however it is useful for staff to be alive to them as ML issues:

- Is the customer located in a high risk jurisdiction, or are there any other geographical risks
- Is the customer employed?
- Are they seeking to play gaming machines with large sums of money?
- Is the customer gambling significant amounts of money and has a lavish lifestyle with no visible means of legitimate support?
- Is the family wealthy?
- Have they been in prison, if so, did their lifestyle continue as before, after being released?
- Are they known to have criminal connections?
- Is there any local knowledge (newspaper articles, gossip, etc.) that may indicate their

involvement in criminal activities?

- Is there any background knowledge about the customer that would give concern?
- Who do they talk to in the arcade?

In the event the member of staff has any concerns as a result they must report the customer to the Nominated Officer (Dobromir Baltadzhiev) and continue to monitor the customer, being careful not to commit the offence of 'tipping off'. This monitoring must include making notes in the customer observation log.

The Nominated officer (Dobromir Baltadzhiev) must then assess the situation and make a decision as to whether a SAR should be submitted, the business relationship with that customer should be terminated, conduct Enhanced Due Diligence, conduct Basic Due Diligence or to continue monitoring.

## **8 CUSTOMER MONITORING**

Chongie Entertainment UK Limited will record any concerns they have with its customers by using the data provided for its own internal records. This is detailed in the Compliance Pack and the Customer Interaction Policy. Customer interactions are recorded on the tablets on site and in the cloud.

The Customer Interaction policy further sets out who staff must escalate a matter to if they have any concerns. The company's Nominated Officer is Dobromir Baltadzhiev and all staff are aware of this.

Any assessment of a customer for Money Laundering purposes will also include a Social Responsibility assessment of the customer in line with the Social Responsibility and compliance Pack and Customer Interaction Policy.

## **9 SYSTEM CONTROLS**

General system controls exist to mitigate the risk of our products and business being used from a POC or ML perspective, and create an environment in which suspicious activity may be effectively detected.

### *Cash Handling*

Location specific operating policies and procedures may be put in place with regards to accounting practices and record keeping, in particular in respect of the following:

- Monetary stakes
- Customer refunds (due to machine malfunctions)
- Money removed from machines
- Ticket in ticket out functions

This is not an exhaustive list and the risks of each location will be analysed.

The cash at each Adult Gaming Centre will be collected and stored in a safe. The external cash collection will take place every 7-10 days. Adult Gaming Centre managers/assistant managers are

required to send an email confirmation to the senior team and attach a signed copy of the customer receipt as soon as the external cash collection takes place. Managers are also required to maintain a special external cash collection log, which must be presented to the senior team in an unlikely case of cash discrepancies investigations or ad hoc spot checks.

External accredited auditors check the CEL cash handling policies and do an unannounced Adult Gaming Centre collection spot check to supervise the process once a year during the annual external audit. Takes place once per annum during our annual external audit.

TiTo software is installed on all category B3 and C machines across the CEL estate. most machines.

A system control has now been implemented on the machines to alert Senior Management if a customer inserts £300 with less than 10% game play. The system operates as follows:

- Senior Management receives an email notification with the following information (by way of example):
  - Type: VTP\_DEPOSIT  
Details: 34.00 / 360.00 = 9.44% (VTP/Deposit Alert)  
Asset number: [xxx], Machine name: [xxx]  
Serial No.: [xxx]  
Adult Gaming Centre name: [xxx]  
Company name: [xxx]  
Time: dd/mm/yyyy 00:00:00 GMT
- Senior Management will review each notification and the corresponding CCTV. In the event it is deemed a high risk transaction or an immediate threat, for example multiple notifications in a short period of time, or an unusually high value transaction, they will investigate as soon as practically possible.
  - If Senior Management calls the Adult Gaming Centre they discuss the situation and make a decision on the outcome, which will usually result in the customer being barred (all staff are trained on the offence of tipping off) or a SAR being submitted to the NCA by the MLRO.
- If Senior Management does not assess the notification to be high risk, the notification will be analysed in due course. This can be done using CCTV, Customer Interaction logs and conversations with the staff on duty. This analysis has several outcomes:
  - No further action (for example if the customer simply moves between machines)
  - Further monitoring, with customer interaction procedures to be initiated
  - Area Manager to be called if customer returns to assess the situation
  - Banning the customer
  - A report to the MLRO, or a SAR reported by the MRO to the NCA

Senior Management will remain in constant communication whilst any interactions are taking place and guide the member of staff through.

All staff members are aware of the offence of tipping off.



## **10 PROACTIVE ANALYSIS**

Senior management proactively analyse the Chongie Entertainment UK Limited's Adult Gaming Centres and the industry as a whole and are always aware of potential or arising problem areas. Senior management monitors the data recorded and keeps up to date with industry news to look out for any abnormal or concerning issues arising. This ensures they are able to be proactive and continue to adopt best practice across all areas of the business.

## **11 SUSPICIOUS ACTIVITY REPORTS (SARs)**

POCA requires SARs to be raised to the NCA in the event of knowledge or suspicion of the use of the proceeds of crime.

A SAR will be raised with the NCA by the MLRO/Nominated Officer (Dobromir Baltadzhiev) or appropriate deputy as soon as is reasonably practicable where suspicion is held that the customer is engaged in money laundering.

A Defence Against Money Laundering (DAML) request can be made to the NCA if the MLRO suspect that continuing with a transaction might involve money laundering.

## **12 SAR MONITORING AND TERMINATION OF CUSTOMER RELATIONSHIPS**

If the level of concern leading to the SAR is maintained in future transactions or has increased thereafter, then further SARs will be considered.

Chongie Entertainment UK Limited understands that SAR reporting and the defence of making a disclosure under section 338 of POCA is not intended to be used repeatedly in respect of the same customer.

Wherever knowledge or suspicion exists, the Nominated Officer (Dobromir Baltadzhiev) will make an assessment with regards to the continuation of the customer relationship. This decision is made with awareness of the potential offences under POCA if transactions are allowed to continue where knowledge or suspicion exists.

In accordance with Gambling Commission guidance, advice may be sought from the NCA around the most effective approach in respect of terminating a customer relationship.

Where a relationship is terminated, steps will be taken to uphold this as effectively as possible.

## **13 PREJUDICING AN INVESTIGATION (TIPPING OFF)**

Staff are trained that subsequent to a report to the Nominated Officer (Dobromir Baltadzhiev), or a SAR being raised with the NCA, it is a criminal offence under section 342 of POCA to release information about the knowledge of the existence of an investigation that may prejudice that investigation.

The Nominated Officer (Dobromir Baltadzhiev) will work particularly closely with customer facing staff to ensure that investigations are not disclosed when a payment is being held pending consent,

or during the process of ceasing the relationship with a customer.

## **14 ADVERSE INFORMATION & POLICE INVOLVEMENT**

### *14.1 Previous Convictions or Previous Police Involvement*

Where information is obtained which indicates previous Police interest or convictions for a financial crime or related offence, a file will be created and steps may be taken to gather customer information from the stages above. Where concerns remain, the customer may be requested to provide proof of identity and source of funds.

### *14.2 Current Police Investigation*

All relevant Police requests for information are logged and a file is created in respect of customers subject to the enquiry (where a file does not already exist), and information provided.

If Police request information in respect of a financial crime enquiry, contact will be made to understand the current status of the investigation.

Provided that the following criteria are met, and there is no overriding knowledge of laundering activity, Chongie Entertainment UK Limited will support and formally cooperate with the Police if there is an explicit request to continue business to preserve the case and evidence.

- The Police must submit a Data Protection Act request for information;
- A formal timeframe for engagement must be established with Police;
- Assurances must be provided by Police that there is a formal investigation, and that the case will be subject to regular review dates. RIPA authority (to provide Police with investigatory and surveillance powers) must be obtained within the first 28 days of engagement;

A Disclosure may be made to the Gambling Commission to advise.

Suspicious Activity Reports will be considered by Chongie Entertainment UK Limited at the point of Police engagement and at each subsequent Police review date.

This cooperative approach seeks to help to ensure that crime is kept out of gambling in the longer term.

## **15 INTERNAL RISKS**

The internal risks of an Adult Gaming Centre include, but are not limited to, the following:

### **Money lending**

Chongie Entertainment UK Limited recognises the risks presented by customers who may seek to transfer money to other customers or third parties or receive funds from other customers or third parties. In order to mitigate this risk, identified transfers between customers and third parties must be assessed by senior management who must satisfy themselves that systematic, organised or commercial money lending is not taking place. Staff will be trained on identifying factors to look

out for and customers may be banned if it is discovered that money lending is taking place.

### **Collusion**

Collusion can be the agreement between people to act together secretly or illegally in order to deceive or cheat someone. Chongie Entertainment UK Limited are aware of the risks collusion present to both the Adult Gaming Centre and in the context of money laundering and proceeds of crime. All staff are trained to be aware of the signs of collusion and to report such signs to management immediately.

### **Machine Fraud**

Machine fraud is an ever present threat and all staff must be aware of the ways in which fraud can take place and what to do in the event they spot a customer defrauding a machine.

Management will ensure the Adult Gaming Centre floor is never left unattended and that customers who are not known, or with whom the staff are not familiar with, are given due consideration. The Senior Compliance team subscribe to the BACTA Crime Bulletin and receive information and photos of known fraudsters on a regular basis. They ensure that photos of known fraudsters are available to all members of staff. Staff must take special care to be aware of situations where large amounts of credit are being played with, machines are regularly going empty, suspicious activity such as large numbers of customers entering a Adult Gaming Centre trying to distract employees takes place and customers covering parts of machines.

In the event a machine is defrauded, floor staff must inform a manager immediately. Employees must take care not to endanger themselves when dealing with a fraudster.

## **16 CUSTOMER DUE DILIGENCE AND ENHANCED DUE DILIGENCE**

Staff must approach customers on a risk based approach. This may differ between Adult Gaming Centres and will be informed by the Money Laundering Risk Assessment, which is required under LCCP 12.1.1, and the Local Area Risk Assessment.

The customer due diligence includes:

- Name, verified with ID such as a driving licence or passport
- Address, verified with ID as above or a utility bill no older than 3 months This must be recorded on the AML portal on the IHL tablet

### **ENHANCED DUE DILIGENCE**

Staff must approach customers on a risk based approach. This may differ between Adult Gaming Centres and will be informed by the Money Laundering Risk Assessment which is required under LCCP 12.1.1.

A customer may require enhanced due diligence if the Nominated Officer (Dobromir Baltadzhiev) deems it appropriate in the circumstances, or if a member of staff, having consulted with senior management, deems it appropriate in the circumstances. Enhanced due diligence can only be carried out by the Area Manager or above. The EDD process will always be supervised either by the CEO or the COO as well as the MLRO.

Enhanced Due Diligence may be carried out on any individuals based in or with strong connections to a high risk jurisdiction.

Enhanced Due Diligence is likely to vary between customers but should normally include:

- A secondary piece of ID
- A recent Bank Statement
- Source of Wealth
- Background checks using open sources such as World Check

This must be recorded on the AML portal on the IHL tablet.

Staff must ensure they also consider the behaviour of established customers when deciding when enhanced due diligence may be appropriate.

In the event there is increasing level of suspicion of money laundering, or even actual knowledge of money laundering, the MLRO must be alerted immediately and a decision made on a case by case basis whether or not the customer may be allowed to continue gambling, whether the MLRO must be notified or whether any other action is to be taken. The MLRO will then decide whether a SAR is appropriate. The MLRO is Dobromir Baltadzhiev.

## **RECORDING**

All customer due diligence and enhanced due diligence interactions must be recorded not only on the AML portal, but also the Customer interaction portal on the IHL tablet.

Further, these interactions must be monitored and reviewed monthly in order to ensure that any patterns emerging are noticed and dealt with if appropriate. This review must be conducted by senior management.

Should the customer refuse to provide the requested documents the business relationship with the customer will be terminated and the customer banned.

## **16 TRAINING AND SCREENING**

Chongie Entertainment UK Limited are committed to ensuring that all key staff understand their responsibilities in respect of POCA and this policy, including internal risks, and in particular the triggers to be alert to and the requirement to report concerns, knowledge, or suspicion to the MLRO/NO immediately.

Staff are trained as follows:

All employees of Chongie Entertainment UK Limited are required to undertake and complete AML training and understand our policy and reporting processes.

### *Head Office*

Key customer facing head office staff, including the Nominated Officer (Dobromir Baltadzhiev), are required to understand and adhere to the Company's POCA & AML policy.

Training refreshers will be held every 6 months and new starters are trained upon induction. Ad

hoc training sessions may be provided to react to developing risks in particular areas.

Furthermore, spot checks take place at all Adult Gaming Centre by members of the Senior Compliance team. These can range from 'mystery shopping' to a series of basic questions asked whenever a member of the team attends the Adult Gaming Centre.

Any weakness identified in staff knowledge are then addressed with additional training or an Improvement Form as part of the HR Disciplinary process.

## **17 MONITORING THE POLICY**

To ensure that the policy continues to be fit for purpose:

Chongie Entertainment UK Limited are committed to carrying out an ongoing risk assessment of its POC & ML regime, tailoring this policy and training around new products and newly identified risks as appropriate.

In the course of day to day activities and in reaction to any POC or ML cases, Chongie Entertainment UK Limited will continue to seek best practices and new techniques to improve the processes and procedures in place.

This policy is subject to review following any new guidance published by the Gambling Commission.

### **Document review:**

<b>Date Reviewed</b>	<b>Reviewed by</b>
05.05.2021	Woods Whur
08.03.2022	Dobromir Baltadzhiev
10.03.2022	Joanne Craig
14.03.2023	Joanne Craig
31.03.2023	Dobromir Baltadzhiev
12.04.2023	Woods Whur
18.04.2023	Dobromir Baltadzhiev
17.05.2023	Woods Whur/Dobromir Baltadzhiev
13.08.2024	Woods Whur/Darren Hughes
05.12.2024	Woods Whur/Darren Hughes
23.12.2024	Dobromir Baltadzhiev
23.04.2025	Woods Whur