| | |
|---|---|
| Document ID<br>**UK_AMK** | **SCHLEP Games UK LTD AML Policy**<br>Print Date:<br>**Sept. 22nd, 2022** |
| Revision<br>**1.1** | Approved By:<br>**Philip Caleb (CEO)**<br>Approved Date:<br>**Sept. 22nd, 2022** |

# SCHLEP Games UK LTD AML Policy

## Policy

GullyCricket engages in several activities to ensure that its operations are not a source of crime and disorder, being associated with crime and disorder, or being used to support crime. The following are the main concrete steps we take to promote the first licensing objective.

1) To Ensure that appropriate measures are taken so that all relevant employees are made aware of the law relating to money laundering and terrorist financing, we have twice anual comprehensive **AML/ATF training**. After the group training session, employees are required to complete an assessment to sufficiently provide they are up to date on all necessary information. This training primarily covers how to recognise and deal with transactions and other activities which may be related to money laundering or terrorist financing.

2) To ensure the **Identification and scrutiny** of complex or unusually large transactions; or unusual patterns of transactions which have no apparent economic or visible lawful purpose; we have a suspicious transaction monitoring program which includes both manual and software components. For example, we use software to determine if certain users are transacting suspiciously and then use manual review and monitoring of those accounts to determine further action. Furthermore, anything suspicious that we see manually through data analysis, customer support interactions, user verification, etc. can cause a user to be included in our "suspicious transaction" monitoring program.

3) We do not allow a **politically exposed person** to use our services. More details on how we identify potential PEP/HIO is outlined in the form of a complete policy in a section included below.

4) To mitigate risk, we do not allow users to transact whatsoever with **cash and cash equivalents, nor do we ever give any type of line credit to users whatsoever.**

5) **Affordability Checks** are in place which would make sure that customers are not gambling beyond their means and also to prevent them from gambling with what may be the proceeds of crime, or to use gambling as a way of laundering money. Specifically, any user who is transacting large amounts will be subject to an enhanced due diligence process. This enhanced due diligence process includes, but is not limited to, verifying the user's source of funds, verifying the user's occupation and industry via open source searches (Google, Linkedin, etc.), following up with the user for any additional information depending on our findings. This also helps us **establish that the customer is using legitimate funds,** as the verification of source of funds and job and occupation information provides sufficient evidence to prove both a user's means and legitimacy of funds.

6) To ensure our **Customer interaction** minimizes the risk of customers experiencing harms associated with gambling, we use software to automatically flag users if their behavior is consistent with problem gambling (this is based on net-loss amount, deposit amount, or betting amount. Ie. having a high threshold in any given time period for any of these three measures would cause you to be flagged). We then prominently display to the flagged users responsible gaming information and links, including information on setting limits each and every time the user tries to further fund their account. We continue to monitor users flagged as potential problem gamblers, and based on a variety of factors, including continued behavior monitoring and information on source of funds and means, we may decide to either limit the user on our end, or end our relationship with that user. In addition, we discontinue any business relationship with a customer if we have money laundering concerns.

7) Our internal policies and training will ensure that **suspicion of offenses** will be promptly reported to the Commision via the online reporting portal with respect to criminal offenses like cheating at gambling or reporting other key events which could have a significant impact on the nature or structure of the business.

8) In order to ensure that customers do not place and layer criminal proceeds through gambling transactions, we **link the payout of winnings with the means by which a customer pays** for gambling transactions. For example, we allow direct bank payments for deposit and will only send withdraws to that same bank, or any other bank which we have verified as belonging to the user and which has been used to deposit. The same goes for all of our payment methods, as all of our payment methods can be used for both deposits and withdraws (for example, Paypal).

## Purpose

Ensure SCHLEP Games will be protected from being a source of crime and disorder, being associated with crime and disorder, or being used to support crime.

## Scope

Each employee involved in the monitoring or verification of users for the purpose of determining AML/ATF risk, as well as each employee in senior leadership, regardless of department, is required to complete the aforementioned training.

There are a few compounding factors that could subject large and/or complex transactions to further scrutiny, however, in general, large transactions completed by relatively new users, unusual patterns of transactions, and/or any indication of cheating, acting on behalf of a third party, collusion, etc. are the main types of indicators that will cause a transaction to be subject to further scrutiny

No politically exposed persons are allowed to use our services under any circumstances.

No cash transactions are allowed under any circumstances.

Every user is subject to the responsible gaming measures described above.

All suspicious offenses will be reported to the commission.

Given that all of our payment methods allow both pay-in and pay-out options (such as bank transfer and Paypal) all users will need to use only a verified pay-in method to withdraw their funds.

## Responsibilities

Our Leadership Team is Responsible For: Fully understanding and also leading AML/ATF Training

Our Legal Team is Responsible For: Fully understanding and also leading AML/ATF Training

Operations Team is Responsible For: Fully understanding and completing the AML/ATF Training

---

## Policy

To identify PEPs, GullyCricket engages in several activities like following adequate due diligence processes, using reliable documents to confirm identity, and screening against specific PEP databases. If the user;s transactions are considered as high risk, enhanced due diligence (EDD) measures are undertaken in order to ensure that PEPs are not allowed access to our app. The following are the main concrete steps we take with regard to the same.

1) **Self-Identification of the Customer**- During sign up, we ask the user themselves if they are a PEP or HIO and we include a definition as to what this is on the sign up page to inform users. If the user is indeed a PEP or HIO, we block that user from using the app, as we do not want to expose ourselves to the increased risk.

2) **Internal Verification of the Identity**- Beyond that, before any user can transact with Money in any way on our app, we verify their identity via collecting a form of government

issued Identification. Using the information we gather on this government ID, we perform open source internet searches and consult relevant reports and databases on corruption risk published by specialized national, international, non-governmental and commercial organizations to try and gather more information on the user, including, among other things, trying to determine if the user is a PEP/HIO. Through these steps we ensure that we are reasonably satisfied that the customer is who they claim to be.

Further, taking into account that the range of PEPs is wide and constantly changing, we **keep ourselves alert to public information** relating to possible changes in the status of our customers with regard to political exposure. This includes, among other things, being aware of if funds are being received from a government account, or if we receive correspondence on an official letterhead from the customer or a related person. Furthermore, if any other interaction with the customer, or information gathered on the customer leads us to suspect they are a PEP, we will terminate the relationship. These interactions could include: A general conversation with the customer or related person linking the person to a PEP and news reports suggesting that the customer client is a PEP or is linked to one.

3) **Enhanced due-diligence based on residence**- Lastly, we ask users their country of residence when signing up. If the user is from a High risk country, as defined below, we undertake **Enhanced due-diligence**:

a) Albania

b) Barbados

c) Botswana

d) Burkina Faso

e) Cambodia

f) Cayman Islands

g) Haiti

h) Jamaica

i) Malta

j) Mauritius

k) Morocco

l) Myanmar

m) Nicaragua

n) Pakistan

o) Panama

p) Philippines

q) Senegal

r) South Sudan

s) Syria

t) Uganda

u) Yemen

v) Zimbabwe

**Enhanced due-diligence** includes taking steps to verify the user's source of funds and **monitoring their transactions** continuously. We ensure that funds paid into the client account come from the account nominated and are for an amount commensurate with the client's known wealth. If they are not, we make sure to inquire about the same. This allows us to further determine if the user is potentially a PEP/HIO, or if the relationship with the user is potentially risky. If we find this to be the case, we will no longer allow such users to use our app.

## Purpose

Ensure that SCHLEP Games undertakes customer due diligence (CDD) and enhanced due diligence (EDD), where needed, so as not to allow politically exposed persons (PEPs) to have access to our services.

## Scope

Every single user is subject to the identification described in the policy and users who wish to transact with money in any way on our app, first have to undergo verification using government ID, which is then used in conjunction with open source searches, so that we are reasonably satisfied that the customer is who they claim to be. All users from high-risk countries are subjected to Enhanced Due Diligence measure.

## Responsibilities

Our Tech and Product Team is Responsible For: Implementing and testing the software necessary to verify IDs and to enable our ops team to perform the aforementioned due diligence and enhanced due diligence, where required.

Our Legal Team is Responsible For: Cotifying policies and internal SOPs necessary to ensure we perform a satisfactory level of customer due diligence and enhanced due diligence, where required.

Operations Team is Responsible For: Performing the diligence checks described in the policies above.

## Policy

Our **Enhanced Due Diligence Process** Is a process through which we obtain more information from any user who we deem **“High Risk”** based on our risk assessment scoring system. We obtain this information by

1) Blocking access to a users account until the submit further verification information
2) Collecting information via open source searches and/or searches on other available resources on the user

Once a user is deemed **“High Risk”**, we first block access to their account until they submit further verification information regarding their source of funds. The user will not be able to access the app until they submit this information.

Once this information is submitted on the users end, the user is added to our **Backend Enhanced Due Diligence Page**, which allows for our operations and compliance team to take the necessary steps on their end to track the users activity and complete our enhanced due diligence process. On this web page, our compliance team is able to see the following information for the High Risk player in question:

1) All user sign up/verification information that they submitted, including source of funds, and links to their ID and address documents
1) Date of the last time this player was risk assessed
2) The User’s Confirmation of source of funds.
3) Confirm players' activities are continuously monitored. (Our Compliance and ops team must confirm they are consistently monitoring this player’s activities)
4) Confirm player’s information is up to date. (Our Compliance and ops team must confirm that they have done open source checks on the backend to confirm the players information is up to date)
5) Documentation of results of open source search of occupation. (Our compliance and ops team must search linkedin and google to try to confirm the users occupation. They type in the user's name and also the occupation the user has given to us to confirm this info is accurate and up to date. They then use any information they find to see if there is any adverse news about this player, or if anything concerning or out of the ordinary arises. They then document the results of this EDD process.)
6) Documentation of the date this EDD was performed

If at any point, based on the Enhanced Due Diligence process compliance finds that this player is either:

a) Intentionally providing inaccurate information.
b) Has reason to believe that this player's history, provided information, or anything else discovered in the enhanced due diligence process suggests that this player is using the app for suspicious and/or prohibited means.

We disallow this user from continuing to play

**The results of this EDD are saved and retrievable at any point in time in the future, if needed, and CAN NOT be edited**. For example, if a high risk player remains high risk for 3 years, and is active all those years, they will have several different "EDD" reports on them saved. You can save these in a separate database or something like that if desired.

---

## Policy

Our **Risk Assessment** process defined a risk score for each user, and based on these risk scores, places the user into three categories:

1) Low Risk = 3.5 and below
2) Medium Risk = 3.51-6.0
3) High Risk = 6.01 and above

A user can also be defined as "Auto high-risk" based on meeting the criteria of only one factor which we find to be enough to cause this user to be high risk. These user's risk scores will automatically be scored as 6.01, regardless of the rest of their risk factor scores.

These risk scores are based primarily on the users transaction behavior, though there are other factors that contribute to a users risk score.

Each player's risk score will start at "**0**" and will increase by a numerical value based on if they meet certain conditions. Most conditions that contribute to a player's risk score can change as frequently as each month, so each month, a player's risk score is recalculated and potentially be updated. There are also other triggers that require us to recalculate certain player's risk scores more frequently.

**Here's How to assign a risk score to each user:**

1. **Country of residence.**

- If they are from a high risk country, we will automatically designate them as **“Auto High Risk”**

- If they are from **Iran** or **North Korea**, we will **permanently block them**

- If they are a Non-UK resident but are NOT from a “high risk country” they will get a risk score **increase of 0.45**

**High Risk Countries:**

High risk countries are
1 Albania
2 Barbados
3 Botswana
4 Burkina Faso
5 Cambodia
6 Cayman Islands
7 Haiti
8 Jamaica
9 Malta
10 Mauritius
11 Morocco
12 Myanmar
13 Nicaragua
14 Pakistan
15 Panama
16 Philippines
17 Senegal
18 South Sudan
19 Syria
20 Uganda
21 Yemen
22 Zimbabwe

### 2. Occupation

If a user has a **high risk occupation**, this needs to be flagged upon them entering their occupation during sign up (however no risk score will be assigned). IF **at any point their lifetime deposits reach $5,000 or more**, they will be designated as **“Auto High Risk”**

High Risk occupations are as follows:

a. Jeweler (manager level or higher)
b. Pawnbroker (manager level or higher)

c. Convenience store owner
d. Restaurant Owner
e. Tobacco distributor (manager level or higher)
f. Foreign exchange (manager level or higher)
g. Money transmitter (manager level or higher)
h. Automotive dealer (manager level or higher)
i. Real estate broker (manager level or higher)
j. Retail store owner
k. Liquor store owner
l. Cannabis store owner
m. Vending machine operator (manager level or higher)
n. Privately owned automated teller machines (manager level or higher)

**3. Deposit/Entry Transaction factors**

- If in the LAST COMPLETED CALENDAR MONTH *(For example, if the score is calculated on august 10th, we must look at the entirety of JULY to decide whether this applies for their current risk score)*
  **the player deposited more than $30,000**, they will get a risk score **increase of 2.4**

- If deposits from 2 months ago was between $5-$10,000, but in the LAST COMPLETED CALENDAR MONTH, the player deposited **more than $29,999**, they will get a risk score **increase of 1.6**

- If deposits 2 months ago was less than $5, but deposits in the LAST COMPLETED CALENDAR MONTH was **more than $10,000**, they will get a risk score **increase of 0.8**

- Entered **Less than $5** in contests (including not entering any contests), or **entered $0** in contest in the LAST COMPLETED CALENDAR MONTH, after having depositing more than $10,000 2 MONTHS AGO
  (*For Example: If I deposit $10,001 in July, then enter any amount $5 or less worth of contests in August, I qualify)* they will get a risk score **increase of 0.8**

**4. Other Transaction factors**

- Players changed (or added) bank account details for deposit/withdraw **(3) OR MORE times in six months**. The way to track this is, check the LAST 6 CALENDAR MONTHS to see how many different bank accounts the player used for interac deposits or withdrawals. If the answer is 3 or more, then the user would be affirmative for this risk factor. they will get a risk score **increase of 0.8**

- If a player has **exactly ONE STR** filed in the past 24 months they will get  a risk score **increase of 0.45**

Once a user is deemed **"High Risk"**, we first block access to their account until they submit further verification information regarding their source of funds necessary for **Enhanced Due Diligence.** The user will not be able to access the app until they submit this information.

Once this information is submitted on the users end, the user is added to our **Backend Enhanced Due Diligence Page**, which allows for our operations and compliance team to take the necessary steps on their end to track the users activity and complete our enhanced due diligence process.

## Policy

Our **Transaction monitoring controls** are based around the tracking and investigation of **"Suspicious Transactions"** and the filing, where necessary, of **Suspicious Transactions Reports (STRs)** to the appropriate regulatory authorities, in this case, the UK Gambling Commission.

To identify suspicious transactions, we use a combination of **automated and manual flags** to flag behavior that we find potentially suspicious. Each transaction that is flagged is associated indicator with an risk indicator based on the flag itself, ie. Flagging a transaction will flag that transaction as either "Low risk", "Moderate risk", or "Extreme Risk", to help further organize and understand the necessary steps associated with each suspicious transaction. Once a transaction has been flagged, the details of said transaction is added to our **Suspicious Transaction Monitoring Web Page**, where our compliance and operations team can further monitor and investigate the transactions, and escalate them as necessary.

**For each Transaction that we flag, a row is created on the STR Monitoring Page with th following columns**:

a) Username associated with the suspicious transaction
b) Date added
a) Reason added
b) Flag creation (Manual/Automatic)
c) Player Risk rating number/ "Automatic high risk" if this applies. ( 3.5 and under in green text. Over 3.5 up to 6 is orange text. Over 6 is red text)
d) Last checked
e) # of indicators (how many STR rows they have **ever** had on this list)

f) Prior STR Reports
g) Notes
h) Add flag

The “username” of each user is clickable. If you click this username, it will open up a new web page that will show the following information about the user:

1. that user's entire **transaction history**
2. ALL of their **verification information**, that they signed up with including sign up date and a link to see their ID.

**Reason added**

The “Reason added” is clickable for each user. IF the user was added manually, then this “reason added” is editable. The Compliance and ops team is able to select a reason from a dropdown list, or select “Other” and type their own answer.

**Last Checked:**

The **“**Last Checked**”** column allows us to keep track of the last time we investigated a player who is acting potentially suspiciously. This column shows a **date** that is clickable.
If we click the date, it opens a pop up that has a button that says “**Checked user?**”. If the ops/compliance resource clicks this button, the “Last checked’ date updates to the date when the button was clicked.

**# of indicators:**

If we click **“# of indicators”** in this list, it brings up a page with the data on all of that user's indicators. There is also the option to **Add User**, where we can search username, email, phone, or user’s full name, in order to manually add players to the STR monitoring list.

**Notes:**

The “notes” column will also be clickable. Anyone can add a note at any time. Notes are date and time stamped, as well as stamped to the actual internal resource who added it.

## When STR Flags are added:

### Low-risk indicators:

**i**f we see activity matching any of the following, the user will be added to the STR monitoring list with a "Low" level indicator. We will monitor the user's account for further action in terms of filing an STR and potentially even blocking that user's account. Low Level indicators ***don't*** automatically mean an STR occurred, but that we need to monitor this user and investigate further.

1. If someone tries to upload one fake ID, we will add a **Manual flag.** If a user tries to upload **2 seperate fake IDs.** We will permanently block this user and file an STR report.
2. Deposits of more than $1,000 within the first week of signing up. **Automated flag.**
3. Deposits of $3,000 or more within the first month of signing up for the **Automated flag.**
4. 3 or more new users in one day sign up and deposit high amounts $500 or more within 48 hours of signing up to the **Automated flag.**
5. 5 or more new users who all signed up in the same week all deposit $500 or more within one week of signing up to the **Automated flag.**
6. 10 or more new users who all signed up in the same month all deposit $500 or more within one week of signing up to the **Automated flag.**
7. We find out a user has successfully created many accounts **Manual flag**

## Moderate indicators:

If we see activity matching any of the following, the user will be added to the STR monitoring list with a "Moderate" level indicator. We will monitor the user's account for further action in terms of filing an STR and potentially even blocking that user's account. Moderate indicators ***don't*** automatically mean an STR occurred, but that we need to monitor this user and investigate further.

1. Users make 5 or more individual deposits within the first 48 hours of signing up to the **Automated flag.**
2. Low or non-earning occupation that does not correlate to the amount of deposits **Automated flag.**

**** Here is how we will define the automatic STR flag of someone who has a low earning occupation that does not correlate to their deposits:*

***Condition 1***

**Any user who has these Industries**

Student (no Field of Occupation Required)
Unemployed (no Field of Occupation Required)
Creative/Artist
Farming

**OR Any user who has this (Industry) + (Occupation)**

(Restaurant) + (General employee)

***Condition 2***

**And ALSO has deposited:**

1) Over $5,000 in one week
2) Over $15,000 in one month

**A user who meets both conditions will get this flag**

3. Player is "high risk" by definition of our player risk assessment **Automated flag.**

4. Player appears to be acting on behalf of a third party or advises the account was Account Created and/or activity initiated under the direction of a third party. **Manual flag.**

5. Player deposits $1,000+ and wants to withdraw ENTIRETY OF UNUTILIZED BALANCE after total entry fees + bets of less than $100 (ie. deposits $1,000 and soon after, request a manual withdrawal, with lifetime bets of $100 or less.) **Manual flag**

6. We find out a user has provided any false information during sign up **Manual flag**

## Extreme indicators:

If a player is found to act in any of the following ways we will file an STR automatically AND we will permanently block their account.

1. Player is found to be a PEP/HIO or the family member or close associate of a PEP/HIO that has been involved or suspected to be involved in criminal activity. **Manual flag**
2. Player refuses to provide a source of funds or provides information that is false, misleading or substantially incorrect or insufficient. **Manual flag.**

3. Player identified by the media, law enforcement and/or intelligence agencies as being linked to criminal activities. **Manual flag**

4. Players using stolen cards **Manual flag**

5. We find cheating or player collusion **Manual flag**

6. Any Attempted collusion with employees in relation to avoiding reporting or verification requirements. **Manual flag**

7. We find out a user has successfully created many accounts AND has been consistently playing against his/her own accounts (done this several times for a large total amount) **Manual flag**

### Other Indicators:

Indicator rating TBD depending on circumstances. If we see any of the following activities, we will also add the user manually to the STR list.

1. Other suspicious looking transactions **Manual flag**

2. Other suspicious looking account verification information **Manual flag**

## Operations for monitoring

### STR MONITORING Procedure:

1. Each user with a “low” or “moderate” STR risk that was added in the past week needs to have their transaction history checked daily.

2. Each user with a “low” or “moderate” STR risk that was added in between 1 and 4 weeks ago needs to have their transaction history checked every 3 or 4 days.

3. Each user with a “low” or “moderate” STR risk that was added in between 1 and 1 month and 3 months needs to have their transaction history checked once a week.

4. Once a user has been on the list for 3 months, but has not been found to be deserving of an STR, they no longer need to be checked regularly, unless they start transacting in a suspicious way again.

## STR Escalation procedure:

1. If a user who is Moderate or Low risk continues to act suspiciously, this needs to escalate to leadership, who will decide If an STR report should be filed with the appropriate authority

2. Leadership will also make a determination, based on the nature of the STR, if the user should be permanently blocked.

---

**Date:** Sept. 22nd, 2022

______________________________
Phil Caleb
CEO