

ANTI-MONEY LAUNDERING (AML) PROCEDURES MANUAL

INDEX

1. Introduction
2. Customer Due Diligence
3. Ongoing Monitoring of Customers' Activity
4. Recognition and reporting of Suspicious Transactions
5. The Compliance Officer's Role
6. Education and Training
7. Recordkeeping
8. Non-Compliance

1. Introduction

1.1. What is Money Laundering?

Money Laundering is the process by which criminals attempt to conceal the true origin and ownership of proceeds derived from their criminal activities, including but not limited to drugs, terrorism, theft, fraud and forgery. When undertaken successfully it allows the money launderer to maintain control over his proceeds and ultimately to provide a legitimate cover for the source of his income. Basically, money laundering is an exercise to take dirty money and make it clean. It is important to keep in mind that the misuse of the trade system is increasingly becoming one of the main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it into the formal economy. Moreover trade-based money laundering may be more difficult to identify and combat.

The Company has adopted Anti-Money Laundering (AML) Program which consists of AML Policy- a document that establishes the main principles adopted by the company to prevent and detect possible money laundering activities and this AML Procedures Manual that sets out a detailed guidance on the implementation of the AML Policy.

1.2 AML Policy Objectives

The principal objectives of the AML Policy are to:

- Prevent The Company from being used by money launderers to further their illicit business.
- Define a framework to enable The Company to assist law enforcement agencies in identifying and tracking down money launderers and their criminal property.
- Ensure that The Company remains compliant with all relevant anti-money laundering legislation and regulations.
- Foster best working practices to protect The Company from financial loss and reputational damage.

These AML Procedures supplement the AML Policy and apply to all the members of the Fraud/Compliance Team and other functions as notified by the company or relevant line managers. Non-compliance by all the employees with the AML Policy and, where relevant, these AML Procedures Manual may be considered as gross misconduct and could result in a disciplinary proceedings.

2. Customer Due Diligence

2.1 Risk Based Approach

The company approach to customers that register an online account and their activity monitoring will be based on the perceived risk profile of the applicant based on the data they provide and/or their activity.

Based on the information collected during the registration and customers' activity (i.e. deposits/withdrawals, betting behaviour, etc.) the Fraud/Compliance Team will classify the customers into the appropriate risk categories (see table below):

Low Risk	Medium Risk	High Risk
Registration details and ID details match and Citizenship/residency confirmed. Age verified	Registration details and ID details don't match and/or Customers that hit any of the thresholds or have suspicious activity in their account (deposits, betting)	Registration details and ID confirmed as invalid after CDD (Customer Due Diligence) or Accounts confirmed with AML issues.

Low Risk

All customers/accounts which are not classified as Medium or High Risk are considered as Low Risk. This includes accounts where manual verification is passed.

Medium Risk

Accounts will be classified as Medium Risk if customers' details do not match, or have any suspicious activity such as deposit pattern, betting activity, account compromised or hit any of our thresholds as described in detail below.

High Risk

Accounts that have been closed for failing verification, Fraud or AML issues are classified as High Risk.

2.2 Customer Verification Procedure

The verification of customer's data is conducted using the details submitted during the account registration by all our customers. The Company Fraud/Compliance Team has 72 hours from the first withdrawal request above a certain threshold made to check the data provided by the customer as follows:

1. ID match

- A. The Fraud Team will compare the registration details entered by any customer during the registration (Full name and ID number) with the copy of ID provided and check for any sign of ID forgery.

Impact of the outcome of the verification on the status of the accounts/required actions:

- **ACCOUNT VERIFIED:** Customer withdrawals are enabled

- **ACCOUNT SUSPENDED FOR WITHDRAWALS:**
 - The details do not match. *The customer will be asked to provide the copy of the ID and the account will stop the withdrawals.*
- **ACCOUNT SUSPENDED FOR ALL ACTIVITY:**
 - The details do not match. *The Customer will be asked to provide the copy of the ID and the account will stop any activity (login, play deposit and withdraw).*

The Company may implement an automated system that will verify the validity of an ID by checking the legitimacy of the document received and cross-checking the ID details with the registration details entered

2.3 Events which trigger additional Customer Due Diligence (CDD)

CDD procedure as described further will apply to the following customers:

- Customers that withdraw more than 2,000 USD/EUR in a single day.

The account will be automatically placed into “SUSPENDED FOR WITHDRAWALS” status (where necessary, the Fraud Team can initiate the manual process for this) and the Fraud Team request proof of ID. Until and unless the ID has been received and confirmed (as described here) the status of the account cannot change.

Once the ID has been received, the Fraud/Compliance Team will take the following steps:

A. Identification Document match – Y or N?

YES: The document received matches the registration details entered by the customer on registration (i.e. names, dob, ID number, expiry date). If the details match, the Fraud/Compliance Team will make a decision based on the ID provided along with additional checks (i.e. social media/internet information) to change the account status to “ACTIVE” with no restrictions.

NO: If the document received does not match the details entered by the customer during the registration, or the Fraud Team has any other reason to question the legitimacy of the document, the Fraud Team will question the customer about the discrepancy of the document compared to the registration’s details with an explanation and/or additional documents to prove it (i.e. Passport, drivers licence, etc.)

The Fraud/Compliance team may decide to perform the Customer Verification Procedure (section 2.2 above) even if the account was successfully verified after the registration.

2. Is the Document legitimate – Y or N?

YES: If the document is legitimate (checks run by the Fraud Team), the KYC status on the account will be changed as “Verified” as long as there are no concerns about the user’s activity in the account.

Note: If the Fraud Team considers it necessary, it can run sanction checks any time.

NO: If the document is not legitimate the account’s status will be changed to “Suspended” and “Not verified” and user requested another proof of ID (i.e. Passport, drivers licence, etc.). Please refer to the Fraud Team procedures for guidance.

All information about the customer’s ID validation will be documented on the account notes.

If, after receiving proof of ID, the Fraud/Compliance Team will inform the Compliance Officer by submitting suspicious activity report according to the AML Policy and this AML Procedures Manual and the customer’s account will be put into “SUSPENDED FOR ALL ACTIVITY” until and unless the Fraud/Compliance team receives instructions from the Compliance Officer as to how to treat the account.

AT NO POINT THE CUSTOMER SHOULD BE MADE AWARE (VIA TELEPHONE, EMAIL OR ACCOUNT NOTES) OF THE REASONS THEIR ACCOUNT FUNCTIONALITY HAS BEEN LIMITED OR THAT INTERNAL REPORT HAS BEEN MADE.

The Fraud/Compliance Team must enter notes related to the results of any investigations in customer's account. These notes will be accessible only by the designated roles within the Fraud/Compliance Team, to be determined by the Compliance Officer.

3. Ongoing Monitoring of Customers Activity

The Fraud/Compliance Team shall monitor and pay special attention to any "Medium risk" and "High risk" Active account and any unusual or suspicious activity in any of the accounts. To do so, the Fraud/Compliance Team will monitor daily customers' transactions in internal backend tools and focus on the following:

1. Deposits/withdrawals
2. P/L (Profit & Loss) on betting activity
3. Multiple payment solutions used in an account
4. Account Registrations (status of the account, KYC, etc.)

The Company considers the following transactions as "unusual transactions" which must be investigated:

1. Those that are shown to be unusual in relation to the user profile;
2. Those in which multiple deposits are made within a short period of time;
3. Those in which large deposits are made, very small bets are placed and large withdrawals/multiple small withdrawals take place.
4. Those in which a large number of different credit cards are used;
5. Those in which several transactions have unsuccessfully been tried to be carried out before it has been confirmed;
6. Splitting-up of bets in order to evade the reportable amounts of The Company.
7. Any repetitive collection of prizes by a same player.
8. Deposit with one payment method and a withdrawal with a different payment method.
9. Players with similar betting patterns.
10. Users with large winnings on different types of games.
11. Change in the living habits of the employees of the obliged operator or that they are denied the taking of holidays.
12. Employees of The Company that use their own address to receive the documentation of the customers.
13. Persons that hide or openly maintain an interest in establishing contact with winners of the games or with employees of The Company.
14. The situation that gives rise to the suspension of the user account as a precaution or the cancellation of the user account for a determined period.

However, the mere carrying out of the aforementioned transactions is insufficient for determining their suspicious nature and on many occasions, a single transaction of those that appear on the list shall not be, by itself, sufficient for determining, with certainty, the suspicion that illegal money laundering activities exist.

At the same time, such activity cannot be left without any action just because there is no certainty of money laundering. If the Fraud Team detects any suspicious transaction that is a result of repeated behaviour as described above, that could be money laundering and they must immediately notify in writing the Compliance Officer of it (see point 4.1 Suspicious Activity Reporting) and put the account into "SUSPENDED FOR ALL

ACTIVITY” status. The Compliance Officer will investigate and will inform the Curaçao Gaming Control Board (GCB) that is tasked with the AML/CFT supervision of the gaming sector operating in and from Curaçao.

The Fraud/Compliance Team can change the account status only upon instructions from the Compliance Officer.

3.1 Account Activity Monitoring

The Company will take a risk-based approach to monitoring and reviewing with the implementation of detailed procedures, which are designed to particular focus upon those accounts and transactions, which are likely to pose the greatest risk from a money laundering perspective (the accounts that are “High Risk” accounts).

The following High Risk accounts will be monitored by the Fraud Team based on the following criteria:

- Single transaction higher than USD/EUR 2,000
- Deposits/Withdrawals for a total of USD/EUR 10,000 in a single month
- Large deposits with minimum betting activity, where the Fraud Team will check large daily deposits and the customer’s betting activity.

Any unusual activity that gives reasons to any member of the Fraud/Compliance Team to suspect possible money laundering must be reported to the Compliance Officer as per Section 4.1 below.

In the event there is no suspicious activity to be reported to the Compliance Office in a given calendar month, designated individual (senior manager within the Fraud/Compliance Team) will submit confirmation to the Compliance Officer identifying the absence of the suspicious activity performed under all accounts.

4. Reporting of Suspicious Transactions

4.1 The Company Employees reporting of Suspicious Activity

The Compliance Officer shall be responsible for the receipt, investigation and disclosure (where appropriate) of all suspicious activity reports.

According to the AML Policy, any staff member of The Company (or a member of staff of The Company’s contractor) who considers any transaction, completed or intended, as suspicious, other than those patterns of customer account activity identified as permitted by the Fraud/Compliance Function, must report it immediately to the Compliance Officer as per AML Policy and in his/her absence to the Legal Representative of The Company. The report has to be made to the Compliance Officer via email:

Compliance@betgr8.com

and include the following information:

- **Email Subject:** ‘Suspicious Activity’ user ID/username.
- **Body of the email:** Explanation detailing why the staff member thinks there is money laundering activity and how it was found. This can include transactions and betting activity related to the account or notes from the conversation or copy of email correspondence.

The Compliance Officer will reply to the staff member with acknowledgement of the email received and with a reference number for the case.

Any suspicious activity reported internally MUST NOT be disclosed to employees, customers, contractor or any other third party.

5. The Compliance Officer's Role

The Compliance Officer's role, in addition to the reporting responsibilities as described above, includes (a couple of examples):

- Implementing and developing the processes within the company through which the AML policies shall be put into practice.
- Working with other departments on assessments of the effectiveness of the AML Policy and AML Procedures Manual and implementing the required changes.
- Keep records related to AML program, internal and external reports and assessments.
- Prepare educational and training materials for the company/employees on the issues of AML.

If you have any questions in relation to The Company AML program, you can obtain more information from the Compliance Officer by sending an email to: Compliance@betgr8.com.

6. Education and Training

All The Company employees, including temporary and contract staff must complete induction training on AML Policy within 30 calendar days of their start date and complete refresher training at least once a year. Staff members are required to demonstrate awareness by passing a knowledge test.

Training may take place using a variety of tools such as electronic learning or face to face.

The training materials and content shall be developed, managed and delivered by the Compliance Officer. The functions dealing directly with the customers and/or customers' accounts will be provided in-depth training on AML Policy and this AML Procedures Manual, including, without limitation, Fraud/Compliance Team.

All The Company contractors which provide any outsourced services to permit The Company to fulfil its obligations pursuant to the applicable laws and/or to provide the services to The Company will be provided with the AML Policy and will commit to comply with the AML Policy requirements. Any such outsourced services that are related to customer face to face or remote communication and/or dealing with customers' accounts activity will be provided with detailed guidance on The Company AML compliance responsibilities including receiving the respective training and this AML Procedures Manual.

The Company will obtain a declaration from all the employees (repeated annually) that they have:

- Read and understood the Anti-Money Laundering Policy;
- Received adequate training in AML;
- Understood their obligations with respect to AML.

The Compliance Officer will hold these declarations in a separate file. HR Department will ensure that all new employees complete the declaration.

The records of all AML training will be maintained and kept for no less than five (5) years.

The Compliance Officer will provide an annual update to The Company Legal Representative of The Company on ongoing AML issues, the effectiveness of The Company AML program and any proposed changes.

7. Recordkeeping

All data, notes, activity and CDD records (ID records, verification and screening records and account transaction history) and all other information related to the account will be kept for the duration of the relationship with the customer and for no less than five (5) years after the relationship has ended (and always in full compliance with

the data protection requirements). This information will be available in The Company platform (backend) under the 'Clients List' tool.

All the records will be completely secure in The Company platform and cannot be deleted.

Records of suspicious activity reports made internally and externally will be kept for five (5) years after the report is made. This should include details of the investigation carried out and the grounds of to the Compliance Officer decision. These reports will be only available to the Compliance Officer (or Legal Representative) who will have easily access via the backend tool via special permission access.

8. Breach of these AML Policy and Procedures Manual

Anyone who knows or suspects any breach of the AML Policy and/or these AML Procedures Manual must report such knowledge or suspicions to the Compliance Officer or, where appropriate, to the Legal Representative of The Company.

Any report or identified breach of the AML Policy or AML Procedures Manual will be fully investigated, in coordination with the HR Department where necessary. Any such investigations of The Company employees' conduct will comply with the local labour laws and will provide for the right of defence of the individual reported. Any disciplinary proceedings will be conducted in strict compliance with the applicable internal policies and laws.

This AML Procedures Manual is subject to the oversight and review on as needed basis and no less than once a year by the Compliance Officer and is not effective without the approval of the Legal Representative of Jack Nickel Integrated Concept Limited

Any new versions of this AML Procedures Manual will be communicated to all The Company staff according to internal policies.

The Company contractors and service providers will be provided with the updated documents within 10 days from approval by the Legal Representative.

Date approved by the Legal Representative of **BG8 Entertainment NV**

Name: PATRICK ROBERTS

Signature: 