

ANTI-MONEY LAUNDERING POLICY

Breakout Group B.V.

Version: 3.0

Effective Date: May 25, 2025

Next Review Date: May 25, 2026

Contact:

compliance@breakoutgroup.com

1. Introduction

1.1. This is the policy of Breakout Group B.V. (the Company) to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities. The Company is committed to complying with all applicable requirements and regulations, including, but not limited to, the regulations of the Government of Curaçao, namely the National Ordinance Reporting Unusual Transactions, the National Ordinance Identification when Rendering Services, and National Ordinance Obligations to Report Cross-Frontier Money Transportations. The Company also adheres to international AML standards set by the Financial Action Task Force (FATF).

1.2. Company's AML policies, procedures, and internal controls are designed to ensure compliance with all applicable regulations and rules. These will be reviewed and updated regularly to account for changes in regulations and changes in our business. Please note that the provisions of this policy also apply to transactions made through the Company's authorized payment agent – HQ BREAKOUT LINE LTD, a Cyprus company, registration number 424448, with the offices located at Vasili Michailidi, 9, 3026, Limassol, Cyprus.

1.3. Please note that the provisions of this policy also apply to the transactions made through the Company's authorised payment agent – HQ BREAKOUT LINE LTD, a Cyprus company, registration number 424448 with the offices located at Vasili Michailidi, 9, 3026, Limassol, Cyprus.

2. Money Laundering (ML)

2.1. Money Laundering (ML) is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other regulated institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Furthermore, the Company distinguishes ML from Terrorist Financing (TF). While ML involves concealing the source of criminally obtained funds to make them appear legitimate, TF is focused on the funding of terrorist activities, which may involve both legitimate and illegitimate sources of funds. The key difference lies in the purpose and origin of the funds: ML hides the source, whereas TF seeks to obscure the destination.

3. Anti-Money Laundering

3.1. Anti-Money Laundering is a financial/legal term used to describe the legal controls that require financial institutions and other regulated entities to prevent, detect, and report ML activities.

3.2. An effective AML program requires a jurisdiction:

3.2.1. criminalization of Money Laundering;

3.2.2. granting the relevant regulators and authorities with investigation powers and instruments;

3.2.3. ensuring that financial institutions and other regulated entities identify their players, establish risk-based controls, keep records and report suspicious activities;

3.2.4. implement ongoing employee training and awareness programs to maintain a well-informed workforce;

3.2.5. cooperate with regulatory authorities and law enforcement agencies as required;

3.2.6. exchange of information with other jurisdictions as appropriate.

4. Regulation

4.1. Employees working in the online gambling industry are required to report any information that comes to their attention in the course of their business when they know, suspect, or have reasonable grounds for knowing or suspecting that a person is engaged in money laundering or terrorist financing, including criminal spend. These obligations are collectively referred to as grounds for knowledge or suspicion. Regulatory authorities expect businesses to demonstrate, with supporting evidence, that a risk assessment has been undertaken before entering into business relationships with players and that adequate player due diligence is conducted to ensure that players' transactions are consistent with the level of risk presented.

4.2. The Company must demonstrate that the extent of ongoing monitoring is conducted on a risk-sensitive basis, and that all records are retained to reflect this, with risk profiles being properly maintained. In this document, the Company outlines additional measures applied to carry out risk monitoring and identify situations where a declaration of the source of funds from players may be required in high-risk situations that potentially involve money laundering.

5. Principles and Practices

5.1. Company's AML policy is based on the following principles and practices:

5.1.1. we develop systems and controls that are appropriate for our businesses and comply with legal and regulatory requirements;

5.1.2. we assess the AML risks inherent in our current business at least annually;

5.1.3. we adopt a risk-based approach that is flexible, effective, proportionate and cost effective;

5.1.4. we have full commitment and responsibility of senior management;

5.1.5. we regularly assess the adequacy of our systems and controls;

5.1.6. we maintain, where necessary, records of transactions that meet the needs of law enforcement investigations tackling money laundering and terrorist financing;

5.1.7. we provide initial and ongoing training for all relevant employees;

5.1.8. we support the nominated officer with resources and authority to operate objectively and independently.

6. Risk Management

6.1. We have a policy and procedures in relation to risk assessment and management, as required under the applicable regulations. This risk-based approach involves a number of discrete steps in assessing the most proportionate way to manage and mitigate the money laundering and terrorist financing risks:

6.1.1. identify the relevant money laundering and terrorist financing;

6.1.2. design and implement policies and procedures to manage and mitigate assessed risks;

6.1.3. monitor and improve the effective operation of controls;

6.1.4. maintain proper recording.

6.1.5. Conduct a documented Business Risk Assessment (BRA), at least annually, to identify ML/TF risks related to the Company's operations, customer base, jurisdictions, and delivery channels. The BRA shall be reviewed and approved by senior management and made available to regulatory authorities upon request.

6.2. This risk-based approach focuses the effort where it is most needed and will have most impact. It has the full commitment and support of senior management as well as active co-operation of all employees. We have conducted an assessment of our business risk exposure to money laundering, which considers the threat, and its impact.

6.3. The Company shall perform a Customer Risk Assessment during the onboarding process to determine the individual risk level of each player. This includes evaluating geographical risk, transaction patterns, employment, source of funds, and potential red flags. The outcome of the CRA will determine the level of due diligence applied.

6.4. Based on the CRA, the Company applies a tiered approach to Customer Due Diligence. Clients identified as high-risk, including PEPs or those from high-risk jurisdictions, are subject to Enhanced Due Diligence. The Company will not onboard clients who fail to provide sufficient documentation or who pose an unacceptable level of risk.

7. Suspicious Activity

7.1. Suspicious Activity refers to suspicious transactions, extreme player profiles, mismatched deposits, and other elements. The implemented proofs of player identity and deposit identification include:

7.1.1. passport or ID card;

7.1.2. utility bill;

7.1.3. bank statement;

7.1.4. source of funds;

7.1.5. proof of income;

7.1.6. proof of payment method ownership.

7.2. The enhanced due diligence checks are subject to players' profile and the risk level they pose to us. Only when we determine some of the above points, or a combination of a few will we flag the player/players in question and conduct risk monitoring. This will include checks of residency, place of work, regular income size and its adequacy to the player spending.

8. Suspicious Activity Reports

8.1. Within the applicable framework, Suspicious Activity Reports (SARs) are an imposed requirement. The Company ensures that any employee reports to the risk team, where they have grounds for knowledge, or suspicion that a person, or player is engaged in ML, or terrorist financing. An employee failing to meet the relevant requirements may be subject to criminal prosecution.

8.2. Escalations of SARs should be done in a confidential, discreet manner, in a handwritten form or any other electronic method provided by law, so as to ensure maximum security and confidentiality of information exchange. An employee must not, under any circumstances, disclose, or discuss any AML concern with the person, or persons subject to an investigation, or any other person for that matter. Disclosure (also known as "tipping off") is strictly prohibited and may result in legal penalties. Furthermore, and in order to keep ourselves protected as much as possible, no remark should ever be left on an account that would give any indication that ML is suspected, a player being entitled, at any point in time, to request the full notes/remarks on their account. Where sufficient grounds of suspicion exist, the Company reserves the right to temporarily or permanently block a player's account and withhold funds pending further investigation or reporting to the authorities.

9. Working Procedure

9.1. Company reviews player's spending and game play to check for suspicious activity. Before any withdrawal is processed the following procedures are carried out:

9.2. The player's deposit history is reviewed to confirm that no suspicious payments have been made to the player's account. The frequency of deposits and the sum of deposits are reviewed to ensure they are within normal range for the player based on his depositing history and the general depositing range throughout our network.

9.3. The player's turnover is reviewed to ensure that they have played in the casino and are not using Company as a method to move money.

9.4. When possible, funds must always be refunded back to the original payment method used by the player to make a deposit.

10. Withdrawal Procedure

10.1. When reviewing a player's account prior to withdrawal the agent must answer the following AML questions in the risk entry:

10.1.1. Did the player wager?

10.1.2. Does the payment method belong to the player and has the player used it to deposit?

10.1.3. Are the player's transactions and bets in line with expectations for the player?

11. Escalation Process

11.1. Following the AML policies in place and escalating any suspicious activity, as previously described, are crucial to the Company as they protect it from financial losses and ensure, that it remains compliant within the different governing jurisdictions. Any activity which appears suspicious has to be escalated. Not escalating a suspicion of money laundering can lead to criminal prosecution.

12. Employees

12.1. Senior Management

12.1.1. Senior management is fully committed to and responsible for the implementation of this policy. Senior management is made aware of their individual personal liability for consenting to, or conniving in, the commission of offenses under the applicable regulations, or where such offense is attributable to any neglect on his part.

13. Staff Training

13.1. All employees are required to undergo comprehensive training on their obligations under this AML Policy, including the identification and reporting of suspicious activities.

13.2. Training must be conducted regularly and cover the following key areas:

13.2.1. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) procedures, including the identification of high-risk clients such as Politically Exposed Persons (PEPs). Screening for PEP status must be conducted at onboarding and periodically during the business relationship. Enhanced due diligence shall be applied where a customer or beneficial owner is identified as a PEP, including: obtaining senior management approval, establishing the source of wealth and funds, and conducting ongoing enhanced monitoring;

13.2.2. Recognition of suspicious transactions and the procedures for escalating such incidents to the Money Laundering Reporting Officer (MLRO);

13.2.3. The legal and regulatory consequences of non-compliance, including potential disciplinary, regulatory, or criminal actions.

13.3. Relevant employees must complete specialized training to ensure proper compliance with AML policies and procedures, including:

13.3.1. Employees must understand and apply CDD procedures, including enhanced due diligence (EDD) for high-risk clients, such as PEPs, in accordance with Curaçao AML/CFT regulations.

13.3.2. Employees are trained to identify and report suspicious activities to the MLRO promptly. This includes obtaining appropriate consent before proceeding with gaming or other business transactions involving suspected funds.

14. AML Compliance Officer

14.1. The AML Compliance Officer is appointed by senior management and is responsible for ensuring the organization's compliance with AML/CFT laws and regulations in Curaçao. Their duties include, but are not limited to:

14.1.1. Developing, implementing, and maintaining the organization's AML program in line with the National Ordinance on AML/CFT.

14.1.2. Monitoring all transactions for unusual or suspicious activity.

14.1.3. Conducting Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) as required by law.

14.1.4. Staying informed about changes in AML/CFT regulations and ensuring the organization's policies are updated accordingly.

14.1.5. Reporting suspicious activities to the Financial Intelligence Unit (FIU) of Curaçao in a timely manner, as mandated by law.

14.1.6. Delivering regular AML training to staff and ensuring they are aware of their responsibilities.

14.1.7. Preparing and presenting reports to senior management on the effectiveness of the AML program.

14.1.8. Ensuring that the organization's operations do not facilitate money laundering, terrorist financing, or other financial crimes.

15. High Risk Jurisdictions

15.1. High risk countries are those respectively identified by the Financial Action Task Force, or other local and international authorities. Client residing in high risk countries are always subject to enhanced due diligence.

15.2. Jurisdictions under increased monitoring currently on the FATF grey list are:

15.2.1. Algeria,

15.2.2. Angola,

15.2.3. Bulgaria,

15.2.4. Burkina Faso,

15.2.5. Cameroon,

15.2.6. Côte d'Ivoire,

15.2.7. Croatia,

15.2.8. Democratic Republic of Congo,

15.2.9. Haiti,

- 15.2.10. Kenya,
- 15.2.11. Lebanon,
- 15.2.12. Mali,
- 15.2.13. Monaco,
- 15.2.14. Mozambique,
- 15.2.15. Namibia,
- 15.2.16. Nigeria,
- 15.2.17. Philippines,
- 15.2.18. South Africa,
- 15.2.19. South Sudan,
- 15.2.20. Syria,
- 15.2.21. Tanzania,
- 15.2.22. Venezuela,
- 15.2.23. Vietnam,
- 15.2.24. Yemen.

15.3. High-risk jurisdictions subject to a call for action (FATF's 'black list') are:

- 15.3.1. Democratic People's Republic of Korea (DPRK),
- 15.3.2. Iran,
- 15.3.3. Myanmar.

15.4. The Company acknowledges that the lists of high-risk jurisdictions and jurisdictions under increased monitoring are subject to updates by the FATF or other relevant local and international authorities. If these official lists are updated, but the Company has not yet reflected the changes on its website or internal documents, the Company confirms that it shall refer to the most recent official updates for the purposes of compliance, risk assessment, and due diligence.

15.5. The Company shall review and update the list of high-risk jurisdictions quarterly, based on the most recent FATF publications and relevant local authority directives. Internal compliance systems must reflect these updates promptly.

16. Record Keeping

16.1. We ensure availability of audit trail to assist in any financial investigation by a law enforcement authority. Our record keeping policy and procedure covers records in the following areas:

- 16.1.1. compliance monitoring by the nominated officer;
- 16.1.2. delegation of AML/CTF tasks by the nominated officer;
- 16.1.3. nominated officer reports to senior management;
- 16.1.4. withdrawal actions by the nominated officer with relevant reasoning;
- 16.1.5. player identification and verification information;
- 16.1.6. supporting records in respect of business relationships or occasional transactions;

16.1.7. employee training records;

16.1.8. internal and external SARs;

16.1.9. communications between the nominated officer and law enforcement authorities.

17. Offenses

17.1. All employees are made aware of their risk of committing the following related offenses:

17.1.1. failing to report suspicious activity;

17.1.2. non-compliance with the disclosure obligations to the nominated officer or respective authority;

17.1.3. disclosure of information about SAR submission that is likely to prejudice any investigation, or disclose information that an investigation into allegations that an offense has been committed, that is likely to prejudice the investigation;

17.1.4. falsification, concealment, destruction or disposal of documents which are relevant to the investigation.

18. Vetting Procedures for New Employees

18.1. The Company undertakes a number of vetting procedures for employment. We will ensure the employee is not a minor through proper identification checks and we will verify the identification and credentials of the employee through at least two independent references. We will also look to verify any further personal information, or background information.

19. Protecting Our Equipment from Internal Crime and Criminal Misuse

19.1. The Company is aware that a key way to combat fraud is to first identify where the company's most valuable assets are. Processes and controls have been built into the routine business of the company to minimize the chances of any of the key assets being misused. Our server equipment is located at secure location, with necessary policies around protection of equipment, for example, a visitors management procedure, fire alarms, shredding of confidential documents, locked cabinets, testing, a security team etc. Same policies are also implemented at Company's offices.

20. Dealing with Trustworthy and Reputable Counterparts

20.1. Company promotes strong principles of business and professional ethics at every level. When selecting business counterparts, the following criteria are considered:

20.1.1. financial strength (for long term sustainability);

20.1.2. legal and regulatory compliance;

20.1.3. commitment to a wider corporate responsibility program;

20.1.4. desire and ability to deliver quality and value.

20.2. All new suppliers must go through a rigorous approvals process where all information put forward by them is verified. This information is then assessed internally to consider the risks associated with the supplier, taking into account all of the above criteria. If rejected, the supplier will be informed. Company ensures, that all organizations we contract with understand the compliance obligations under the relevant player jurisdictions.

20.3. All third-party service providers and business partners must undergo due diligence procedures consistent with the Company's AML standards, including verification of legal status, ownership, compliance track record, and screening against sanction lists.

21. Our Responsibilities

21.1. Company is fully aware of the procedures and policies required by the applicable Laws and regulations and apply related internal policies and procedures.

22. International Record Keeping

22.1. Records on all player transactions regardless of their relation to payments or plays will be kept for at least 5 years after the transaction.

22.2. Records on player details regardless of their value state or open/blocked status will be kept for at least 5 years after the relationship with the player was terminated.

22.3. Records on money laundering investigations and suspicious activity reports will be kept for 5 years after the investigation was completed.

22.4. Records may be retained for longer than five years if required by an ongoing investigation or as requested by regulatory or law enforcement authorities.

23. Prevention of Collusion and Data Protection Compliance

23.1. The Company's Terms of Service make clear that cheating will not be tolerated and that player accounts will be closed if cheating occurs. In terms of data protection, all data related to player payment accounts is stored, encrypted, and Company's employees have no access to player payment information. All player information in the organization will be protected through a strict information security policy that all employees and suppliers will adhere to, that will include system access and authentication control, password policy, malware protection measures, intrusion prevention policy, encryption policy, and strict network control and management.

24. Sanctions Screening

24.1. At our Company, we prioritize compliance and integrity in all our operations. To ensure that we conduct business responsibly, we rigorously screen our clients, suppliers, and employees against relevant sanctions lists, including those from OFAC, the EU, the UN, and other international authorities. This proactive approach helps us avoid engaging with sanctioned individuals or entities.

We utilize a variety of specialized services to support our screening efforts.

Automated services verify the identity of users by collecting and analyzing various identification documents, such as passports and driver's licenses, alongside biometric data and other pertinent information. This thorough verification process enhances our ability to confirm the legitimacy of each individual or entity.

These services conduct comprehensive screenings against global sanctions lists, identifying individuals, entities, and countries that are subject to sanctions or restrictions. This ensures that we maintain a clear understanding of any potential risks associated with our business relationships.

Our automated systems assess the risk associated with each user based on their identity and the outcomes of the sanctions screening. This allows us to identify high-risk individuals who may require additional scrutiny, ensuring that we make informed decisions in our business dealings.

We are committed to ongoing compliance. Automated services provide continuous monitoring to ensure that users remain compliant with sanctions policies over time. This includes regular updates and re-screening as necessary, helping us stay ahead of any changes in sanctions regulations.

The platforms we utilize generate detailed reports and alerts for any issues or discrepancies that arise during the verification and screening processes. This capability enables us to take swift action, such as freezing accounts or conducting further investigations when needed.

We are actively working on integrating these automated services into our Company's existing systems and processes. This integration not only streamlines compliance checks but also ensures that the verification process is seamless and efficient. By leveraging technology in this way, we reinforce our commitment to maintaining high standards of compliance while fostering trust with all stakeholders.

25. Outsourcing and Third-Party Risk Management

25.1. When outsourcing AML-related activities to third parties, the Company will ensure that they also comply with our AML policies and applicable regulations. The Company will conduct due diligence on third-party service providers and maintain ongoing oversight to ensure their continued compliance.

26. Reporting Channels and Incident Response Plan

26.1. The Company will establish clear communication channels for employees to report suspicious activities or incidents related to money laundering, including an anonymous whistleblowing mechanism. An incident response plan will be developed to handle identified money laundering incidents, including steps for investigation, reporting, and remediation.

27. Technology and Software

27.1. The Company will utilize specialized software or technology for risk assessment, monitoring, and reporting as needed. These tools will be kept updated and maintained to ensure their effectiveness in supporting the Company's AML efforts.

28. Independent Audit of the AML

28.1. The Company conducts an annual independent audit of its AML program, ensuring compliance with all applicable laws and regulations. The audit is carried out by the external auditor with the necessary qualifications. Those conducting the audit are entirely independent from the daily operations of the AML program, ensuring an objective and impartial evaluation of its effectiveness.

28.2. The scope of the audit covers key areas, including a thorough review of the Company's AML, CTF and CPF policies and procedures to ensure alignment with current laws and best practices. It also involves a detailed assessment of customer files, including CDD and EDD processes, to confirm that proper identification, verification, and risk management practices are in place.

28.3. The Company's overall compliance management framework is rigorously evaluated, ensuring that governance structures, risk management, and internal controls are operating effectively. Transaction testing is conducted to verify that the Company is adhering to its internal policies and regulatory obligations. The adequacy of AML-related employee training is also reviewed to ensure that employees receive ongoing education on AML compliance responsibilities.

28.4. In addition, the audit evaluates the effectiveness of the Company's transaction monitoring systems in identifying and reporting suspicious activities. Employee interviews are conducted with relevant staff to assess their understanding and application of AML processes. A sample of unusual transactions that meet or exceed established thresholds is reviewed to ensure compliance with internal policies and external reporting requirements.

29. Oversight & Contacts

19.1. In addition, the audit evaluates the effectiveness of the Company's transaction monitoring systems in identifying and reporting suspicious activities. Employee interviews are conducted with relevant staff to assess their understanding and application of AML processes. A sample of unusual transactions that meet or exceed established thresholds is reviewed to ensure compliance with internal policies and external reporting requirements.

29.2. Related Information

This policy must be read in conjunction with the Company's Privacy Policy, Terms of Service, and. It also aligns with FATF recommendations and Curaçao's national AML legislation.

29.3. Contact Information

Questions regarding this policy should be directed to the Compliance officer at:
compliance@breakoutgroup.com

29.4. Policy History

Version 3.0 — Effective Date: May 25, 2025

29.5. Responsible Office

Compliance officer Breakout Group B.V.

29.6. Next Review Date

May 25, 2026