Anti-Money Laundering and Combating the Financing of Terrorism Policy

Hash Games CW B.W.

2024

Table of Contents

1. AML POLICY OVERVIEW

1.1 Policy Objectives and Scope

As part of its continuous improvement implementations, *Hash Games CW B.W.* is dedicated to putting in place the necessary steps needed to ensure that all employees, full-time or contractual, participate actively in preventing any of the Company's services and/or outlets for the sole or partial purpose of money laundering and/or the financing of terrorist undertakings.

Money laundering (ML) and the use of legal or illegal monies for the purpose of terrorist financing, have become ever growing threats - Hash Games CW B.W. (referred to herein as the "Company") is fully committed to playing its role in assisting with the international fight against such organized crime and terrorism.

The Company has therefore incorporated the following Anti-Money Laundering and Terrorist Financing Policy ("Policy") as part of its internal process. The Company has applied this Policy to all its employees and adheres to the highest of the industry's best practices in its mission to prevent any possible criminal activity through money laundering.

1.2 Money Laundering Defined

Money Laundering is the terminology used for a number of illegal offences encompassing money obtained from certain crimes, (such as extortion, insider trading and drug trafficking) as "dirty" and needs to be "cleaned" to appear to have been derived from legal activities, so that banks and other financial institutions will deal with it without suspicion. Money can be laundered by many methods that vary in complexity and sophistication.

The Money Laundering (Prevention) Act, 1996 defines money laundering as:

The concealment of the origins of illegally obtained money, typically by means of transfers involving foreign banks or legitimate businesses. Engaging directly or indirectly, in a transaction that involves money or other property.

Whether it be through conversion, transfer of property, concealment, disguise, acquisition or possession of funds derived from criminal activity or the participation/assistance of the movement of funds derived from criminal activity in order to appear legitimate – are all forms of money laundering.

1.3 Distribution of the AML Policy

This AML Policy has been reviewed and approved by the Executive management team. The Policy is provided to all staff (frontline, leads, managers and The Board) and is redistributed as updated.

The Compliance Officer is responsible for providing a report to the Executive Management team for review not less frequently than once every twelve (12) months as to the effectiveness of the Policy and related operational procedures, and shall provide recommendations to management as to proposed operational or policy enhancements.

The Executive management team shall review the content of this Policy for necessary revisions or updates not less frequently than once every twelve (12) months. Recommendations and feedback will be given to the Compliance Officer.

With the exception of directives from relevant authorities, any proposed amendments to this Policy require the review and approval of the Compliance Officer, the Executive management team, and legal counsel.

2. COMPLIANCE OFFICER – MONEY LAUNDERING REPORTING OFFICER (MLRO)

2.1 Appointment of the Compliance Officer/MLRO

A qualified senior employee shall be appointed at all times as Compliance Officer- also referred to as the *Money Laundering Reporting Officer* (MLRO). The Compliance Officer has been identified and the Compliance Officer's contact details made available to all staff and applicable staff of service providers.

2.2 Reporting Structure and Independence

The Compliance Officer holds no other position within the organization or any affiliated company or supplier and operates independently from all other functions within the organization in order to ensure that actual or perceived conflicts of interest do not occur. Subject to oversight by the CEO, the Compliance Officer has the authority to act independently from other functions within the organization in order to fulfill his/her below noted roles and responsibilities.

The Compliance Officer has the full and public support of the Executive management team in executing their duties. All staff are required to assist the Compliance Officer (and the nominated officer, as appropriate) in fulfilling their duties.

2.3 Duties and Responsibilities of the Compliance Officer/MLRO

The Compliance Officer is tasked with the responsibility of supervising and controlling all compliance-related operations conducted by the organization and its impacted vendors, which includes the implementation of the procedures outlined in this Policy. MLRO/Compliance Officer responsibilities consist of (*but not limited to*) the following:

- Ensure that procedures are in place to ensure compliance with all applicable legislation, regulations and all associated guidelines, codes of practice and Company policies and procedures;
- Report to the CEO and inform senior management the result(s) of any remedial action required and/or taken;
- Update and maintain any compliance-related policies, including this Policy;
- Plan and co-ordinate training activity for all departments to include key regulatory areas including the significance of regulatory compliance as a whole, ID and age verification, fraud, Anti-Money laundering, and problem gambling;
- Be the point of contact with the involved Regulator(s) and the related FIU;
- Investigate and report any breaches of the applicable laws, regulations, guidelines, codes of practice and company policies and procedures to senior management and, as appropriate, to the Regulator;

- Plan and co-ordinate training activity for all departments to include key regulatory areas including the significance of regulatory compliance as a whole, ID and age verification, fraud, Anti-Money laundering, and problem gambling;
- Manage regular reviews of Company's internal control system to ensure that it accurately reflects the then current operation of the business – and report any discrepancies/oddities to relevant senior management.

3. FIRM POLICY AND COMMITMENT

The Company will ensure it has appropriate policies and procedures in place to complement this AML policy, in compliance with applicable regulations and monitoring of adherence to those policies will also take place.

Staff members are trained in AML processes and procedures and will actively participate in preventing the services of the Company from being exploited by criminals for money laundering or terrorist financing purposes. The objectives of this and related policies are:

- Assuring the Company's adherence to all relevant legislation and statutory regulatory instruments;
- Preserving the organization and its personnel from the potential hazards linked to violations of statutes, regulations, and oversight obligations;
- Preserving the good name of the Company against the risk of reputational damage presented by implication in money laundering and terrorist financing activities;
- Making a positive contribution to the fight against crime and terrorism.

4. SCREENING AND MONITORING

4.1 Account Screening

An automated and manual preliminary screening is performed on newly created customer accounts to detect any suspicious or potentially linked activities. Such screening seeks for elements that may be dubious and/or questionable, such as:

- Accounts that may present comparable information;

- At least two accounts that were created using the same email address;
- A customer who possesses multiple accounts;
- Any additional suspicious activity or information that the Fraud or Financial Services teams have identified or suspect.

In the event that any of the foregoing screening identifies potential issues, the Financial Services team is notified automatically and will investigate and apply applicable business rules accordingly. Such business rules may result in a variety of potential risk mitigation steps, including closure of account, escalation to the Fraud team for enhanced diligence, limitation of deposit or withdrawal methods, imposition of deposit limits, etc.

4.2 Enhanced Due Diligence (EDD)

In certain cases, there is the possibility certain customer relationships demonstrate heightened AML or fraud risks to the Company. In such instances and in addition to its regular customer due diligence protocols, the Company shall carry out enhanced due diligence (EDD) processes.

During the enhanced due diligence process, the Company will take additional required steps in order to aid in identifying a potential customer, including (but not limited to) personal and financial background. This may involve obtaining additional evidence in verifying the individuality of the client.

This may include obtaining evidence to verify particular aspects of the customer's identity and verified confirmation in order to establish the source of funds of the customer. The Company's fraud detection agents have access to a variety of tools through its suppliers and databases - which are used to verify submitted documentation (e.g. Drivers Licenses, Passports and various government-issued documents). The circumstances that may trigger additional concern and may require enhanced due diligence (EDD) are noted below:

- The customer or potential customer is situated in a country of territory that does not apply to the Company's geographical market.

- The customer or potential customer is or appears to be a Politically Exposed Person (*see below*).
- Any other circumstances if the Company reasonably perceives to be a heightened risk for money laundering or terrorist financing.

4.3 Politically Exposed Person (PEP)

A *PEP* or Politically Exposed Person, is an individual who currently or previously held a prominent public function in any country. A wide range of persons may be considered as PEPs, including heads of state, senior members of the judiciary, senior military officers and immediate family members of such persons.

A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.

If an account is identified as a potential match to a PEP list, the account shall be immediately frozen pending escalation and review. The Compliance Officer is immediately notified and a further assessment is made. The Compliance Officer will reach out to the appropriate department and offer his/her recommendations regarding the account.

4.4 Reporting

If for any reason the Company reasonably suspects that a client and/or account may be involved in any form of activity that may amount to money laundering, the Company will immediately inform the required and appropriate external authorities.

If the Company believes that some degree of suspiciousness after a transaction has taken place and after an internal investigation confirms as such - the Company will freeze the account and will inform the relevant authorities immediately and disclose the necessary information required by law to do so.

The Compliance officer or an authorized staff member, will take ownership and report the activity through the appropriate AML reporting form and submit it to the Regulator.

Additional reporting procedures are put in place in order to mitigate the Company's exposure to various forms of money laundering. These consist of in-house and third-party reporting/monitoring tools that run daily and/or weekly. Furthermore, AML reporting procedures such as *Suspicious Activity Reporting* (SARs) and *Significant Transaction Reports* (STRs) will be conducted and submitted when needed to the Regulators and if necessary the appropriate law enforcements:

- **Significant Payment Reports (STRs)** – The Company shall implement and maintain an automated system to identify all account withdrawals in excess of a particular amount within a rolling 30 day period ("Significant Transactions"). Reports will be generated within a 48-hour timeframe of payment being made and kept for record purposes and if required, submitted to the Regulator.

- **Suspicious Activity Report (SARs)** – The Company shall implement and maintain an automated system to identify any account that may depict suspicious activity. This may include (but not limited to) gaming activity, transactional behavior out of the ordinary within the account, etc. SARs are to be filled by the Compliance Office/MLRO or authorized individual and submitted to the Regulator.

- **Casino Gaming Reports** – Through the Company's in house security and fraud prevention tools, all activities are tracked which include financial instruments logged and gaming transactions recorded. Reports generated daily will assist in identifying players who may have found an avenue in order to take advantage of a system vulnerability. Once identified and confirmed – the appropriate action on the account takes place.

- **Poker Security Reporting and Tools –** The Company provides customers the ability to engage in online poker play against other players. So called peer to peer games where the funds at risk are the players' and not the house. Due to its nature as peer to peer, transactional game poker does have an inherent risk of money laundering. However, the Company addresses the potential risks with a strict regime of monitoring poker activity with the following tools and reports:

- *Collusion Analyzer*: Collusion tool is designed to prevent collusive activity at ring game highlighting pairs of accounts with game play together. The system security center will flag accounts based on percentage of play together, percentage of raises together, amount won/lost and number of hands. Accounts are flagged by severity levels and are reviewed as needed to ensure legitimate play.
- *Bot Detection*: Bot detection tool is designed to highlight possible accounts possibly using third party software. Accounts are flagged by severity levels and are reviewed as needed to ensure legitimate play.
- *Bonus Abuse Reports*: A review of accounts which have been issued bonuses will validate if the appropriate rollover requirement has been completed – making sure the player has respected all of the bonus terms issued by the Company. Detection will also be applicable to accounts who may take advantage of bonus programs and abuse them through referral incentives.

As noted, the following reports are either generated daily/weekly in order for the appropriate department to review and analyze. Other reports imposed by the Regulator, may require the Compliance Officer/MLRO or authorized individual, to compile and submit in a timely fashion.

4.5 Third Party Supplier Diligence

The Company recognizes that as it contracts or outsources certain functions, the potential exists to create extended AML risk if such third parties are not adequately identified and their applicable processes reviewed.

Prior to entering into any agreement for services in relation to which this Policy applies, the Company conducts “KYC” diligence to establish the corporate bona fides of such potential partners. This diligence includes, at a minimum, securing the following documentation:

- Certificate of Incorporation and Memorandum & Articles of Association;

- Identification of Directors and, if a private company, shareholders;
- Declaration of Beneficial Ownership;
- KYC, as appropriate, of signatories.

In addition, for potential third party suppliers that will provide payment or processing services shall provide a copy of its AML/CFT policies and/or procedures, which shall be reviewed by the Compliance Officer/MLRO and Legal team to ensure that the supplier's KYC processes and AML risk management is satisfactory - having regard to the nature and quantum of the potential AML risk.

4.6 Ongoing and Continuous Monitoring

The Company executes and oversees every action of its clients and/or employees in order to guarantee that every action, whether instructional or transactional, is executed consistently and with the necessary focus to identify potential money laundering or financing of terrorism.

5. EMPLOYEE DILIGENCE

Each Company employee or staff member of a business affiliate or service provider whose role is affected by this Policy is screened prior to being hired or appointed to work on Company tasks.

Company conducts an extensive background check and all prospective employees may be subjected to a credit and criminal record check prior to an offer of employment being made.

5.1 AML Training

Specific training protocols shall be conducted in respect of the Policy to the following functional groups:

- Frontline Staff (customer service)
- Fraud/Investigation employees
- Financial Services
- Management/Senior Management

The Compliance Officer/MLRO is responsible for ensuring that the training modules are accurate and of such a standard as to communicate the requirements of this Policy effectively to the applicable audience(s). The applicable training shall include, at a minimum, guidance as to the identification and reporting of transactions that must be reported to the Compliance Officer/MLRO and examples of different forms of money laundering schemes that could seek to take advantage of Company's business for illegal purposes.

The Compliance Officer/MLRO will supply the appropriate AML training (which may consist of in-class, video conference or literature) in order to provide involved staff, guidelines and direction on:

- The process in reporting suspicious activity;
- The type of activity that should be considered significant and critical in detecting possible money laundering – these may be given in class or reading materials;
- Distinguishing specific incidences that may require cause for re-assessment of a risk-based approached;
- The Company consistently implements monitoring processes with the addition of potentially new and future products and/or services it provides to its clients;
- Implementations and assessments are put in place (and adjusted if need be) in order to mitigate any possible risk of money laundering or terrorist financing where the use of new products and/or services may be vulnerable to. These include (but not limited to):

    - Overview analysis of transactions over specific periods;
    - Overview analysis of new services/products used by the client;
    - Applying limits to activities on new products/services used by the client for a given time;
    - Requests for justification of noticeable irregular activity from the client.

Training participants will be assessed at the conclusion of such training to ensure that the applicable contents of the Policy have been effectively conveyed. AML trainings will be conducted not less than once every twelve months.

The Compliance Officer shall maintain records of which employees have attended and passed the above-noted training protocols, which records shall be maintained by the Compliance Officer/MLRO for not less than six (6) years.

6. MANAGEMENT OF COMPLIANCE AND AML POLICIES

It is the Company's policy to monitor its compliance program with legal and regulatory AML/CFT requirements. The Policy will be reviewed annually and amendments added accordingly when new products and/or implementations are applied.

The effectiveness of the Company's AML/CFT program is regularly evaluated to ensure it remains current and is aligned with business activities, regulatory developments, industry standards and best practices. By doing so, the Company adheres to all applicable laws and regulatory requirements in the jurisdictions in which it operates.

This document has been reviewed and approved in January 2024.