

Anti-Money Laundering (AML) Policy

1. Introduction

1.1 Money Laundering

Money laundering (ML) is the process of concealing the origins of illegally obtained money to make it appear legitimate. This may involve disguising the source, altering the form, or transferring funds to jurisdictions with weak regulatory environments.

1.2 Anti-Money Laundering (AML)

AML refers to the set of legal and regulatory frameworks that obligate financial institutions and other regulated entities to prevent, detect, and report ML activities. An effective AML framework must:

- Criminalize money laundering;
- Equip regulators and law enforcement with investigative powers;
- Require financial institutions to conduct customer identification and risk-based monitoring;
- Enable appropriate international cooperation and information sharing.

2. Regulatory Compliance

All employees in the remote gaming industry are required to report any knowledge, suspicion, or reasonable grounds for suspicion of money laundering or terrorist financing. Risk assessments and customer due diligence (CDD) must be conducted prior to engaging in business relationships, and records must be maintained to demonstrate ongoing monitoring in a risk-sensitive manner.

2.1 Applicable Regulations

The Merchant operates under a Curaçao Gaming License, which authorizes the offering of games of chance in the international market. We are committed to full compliance with all applicable legal and regulatory AML obligations.

3. AML Policy Principles

Our AML framework is based on the following principles:

- Development of appropriate systems and controls;
- Annual AML risk assessment with a risk-based, proportionate approach;
- Senior management commitment and oversight;
- Regular system evaluations;
- Comprehensive record-keeping for law enforcement purposes;
- Mandatory AML training for relevant employees;
- Independence and resourcing of the Money Laundering Reporting Officer (MLRO).

4. Risk Management

In accordance with the Money Laundering Regulations, we maintain risk-based procedures for identifying, managing, and mitigating AML/CTF risks. These steps include:

- Identification of relevant risks;
- Design and implementation of controls;
- Ongoing monitoring and updates;
- Full documentation of actions and rationales.

5. Suspicious Activity Monitoring

We monitor for suspicious behavior, including unusual deposit patterns, mismatches between deposits and gameplay, and other anomalies. Enhanced Due Diligence (EDD) may involve requesting:

- Government-issued ID (e.g., passport);
- Utility bill;
- Bank statement;
- Proof of income or source of funds.

5.1 Suspicious Activity Reports (SARs)

Employees must report any suspicion to the Risk Team. SARs must be submitted securely. Disclosure or discussion of an SAR ("tipping off") is a criminal offence.

5.2 Working and Withdrawal Procedures Before processing a withdrawal:

- Review deposit history for irregularities;
- Confirm gameplay activity;
- Ensure funds are returned to the original payment method, where possible.

5.3 Escalation Protocol

Any suspicion, however minor, must be escalated immediately to the MLRO. Failure to escalate can lead to criminal liability.

6. Roles and Responsibilities

6.1 Senior Management

Senior management is responsible for implementation and compliance with AML policies and is liable for breaches under AML legislation.

6.2 Money Laundering Reporting Officer (MLRO)

The MLRO handles SARs, reports to senior management, and has the authority and resources to act independently.

6.3 Staff Training

All employees receive initial and ongoing AML training, including CDD procedures and SAR protocols.

Relevant employees receive training on how to follow house policies and procedures for:

- Client due diligence (CDD), including enhanced requirements for high-risk clients, which includes PEPs;
- Reporting suspicious activity to the nominated officer where necessary, seeking appropriate consent to allow participation in gaming and to conduct gaming and other business transactions

7. High-Risk Jurisdictions

Clients from countries identified by the FATF or relevant regulators as high-risk are subject to EDD. Customers from blacklisted jurisdictions may be denied service.

Countries currently on the FATF list are:

- Afghanistan
- Algeria
- Angola
- Bosnia & Herzegovina
- Ecuador
- Guyana
- Iraq
- Lao PDR
- Myanmar
- Panama
- Papua New Guinea
- Syria
- Uganda
- Yemen
- Iran
- Democratic People's Republic of North Korea

Players from the FATF list of jurisdictions seen to threaten the international financial system from on-going and substantial money-laundering or terrorist financing activities, as identified on FATF publications, will be refused.

8. Record Keeping

Records are maintained to support audits and investigations, including:

- Compliance monitoring reports;

- CDD documentation;
- SARs and related communications;
- Training logs;
- Internal escalations.

9. AML Offences

Employees may face criminal prosecution for:

- Failing to report suspicious activity;
- Tipping off a customer;
- Interfering with investigations.

10. Employee Vetting

New employees undergo ID verification and background checks, including two independent references.

11. Internal Security Controls

Our data and infrastructure are protected by access controls, visitor management, encryption, and physical safeguards at our Malta-based data center and company offices.

12. Compliance and Risk Committee

A Compliance and Risk Committee, including the MLRO, Compliance Officer, and a non-executive director, meets quarterly to review risk management.

13. Supplier Due Diligence

We ensure that all partners and suppliers are reputable and compliant, assessing them for financial stability, regulatory adherence, and ethical standards.

14. Proceeds of Crime Act (POCA) Compliance

We comply with POCA 2002 and related AML legislation, ensuring our policies reflect statutory obligations.

15. Internal Record Retention

We retain:

- Customer transaction data for 6 years;
- Customer identity records for 6 years post-relationship;
- SARs and investigation files for 6 years after closure.

16. Prevention of Collusion and Data Protection

Cheating and collusion are grounds for account termination. Payment data is managed by Payment IQ and protected by encryption. Our Information Security Policy covers:

- Access control and authentication;
- Password and malware protection;
- Intrusion prevention and network security;
- Data encryption.