



FRAUD MANAGEMENT AND AML POLICY

Table of Contents

1	Introduction	3
2	Objectives	4
2.1	<i>Know Your Client (KYC) and Anti Money Laundering (AML)</i>	<i>4</i>
3	Risk Assessment - Procedure	5
3.1	<i>Product / Service Risk.....</i>	<i>5</i>
3.2	<i>Interface Risk</i>	<i>5</i>
3.3	<i>Geographical Risk</i>	<i>5</i>
3.4	<i>Risk Management Procedures</i>	<i>6</i>
3.5	<i>Tipping Off</i>	<i>6</i>
3.6	<i>Reporting Procedures and Obligations</i>	<i>6</i>
3.6.1	<i>Selection of new employees</i>	<i>6</i>
3.6.2	<i>Awareness and Training to Employees</i>	<i>6</i>
4	Responsibility.....	7

Fraud Management and AML Policy

Version 1.1
Date issued 2023-04-10
Approved by Board of Directors

Revision history

Date	Author	Comment
2022-02-17	JO	First revision
2023-03-17	NJ	Review and update

1 Introduction

Slotmill only provide B2B services and does hence not deal directly with players / end users. Slotmill requires that the Operators we do business with and that are dealing directly with players, are responsible for ensuring that appropriate Fraud Management and AML measures are upheld and adhered to in accordance with this policy. This is in line with the latest AML directives and the MGA&FIAU guidelines including the FIAU implementation procedures.

During the year 2020, two new Anti-Money Laundering (AML) Directives came into force:

1. The 5th AML Directive on the 10th January 2020
2. The 6th AML EU directive on the 3rd of December 2020

The 5th Anti-Money Laundering Directive (AMLD5)

The [AMLD5](#) aimed at strengthening the then-current Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) provisions, and specifically:

1. increase transparency for the ultimate beneficial ownership (UBO) registry.
2. **extend the AML regime into Cryptocurrencies to manage and prevent risks arising from virtual currencies.**
3. harmonization of the application of enhanced due diligence measures from transactions involving the high-risk third countries.
4. limiting the anonymous use of prepaid cards.
5. grant new powers for financial intelligence units (FIUs).
6. ensure the existence of a centralized national account registry.

The 6th Anti-Money Laundering Directive (AMLD6)

The AMLD6 now aims to empower financial institutions and authorities to do even more in their fight against money laundering (ML) and terrorism financing (TF) by:

1. **expanding** the scope of existing legislation,
2. **clarifying** certain regulatory details, and
3. **toughening** criminal penalties across the Union.

The amendments added in the AMLD6 aim for further transparency across the Union and we explain what is coming along with the AMLD6 below:

1.1.1. The provision of online gambling services is subject to national, EU and international regulations and Slotmill has a duty to comply with all applicable laws and regulations in order to maintain its current gambling licenses, be able to successfully apply for additional licenses and protect its own reputation and its partners'. One of the main drivers is to protect its operation from fraudulent transactions. fourth revision of the EU legislative framework, Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing. The Directive is abbreviated as "AML4" throughout this document.

Money laundering may however occur also in B2B activities, and the following examples that potentially can signal such attempts:

- Suggestions to make large payments in cash

- Payments by or via a party is not a party to the contract
- Requests to pay more than provided for in the contract
- Payments made in currencies other than those specified in the contract
- Payments from an unusual, nonbusiness account

If such activity is suspected, it shall be reported to management. Monitoring this is primarily the responsibility of the finance department, and any suspicious activity shall be reported to the CEO.

2 Objectives

Slotmill will be managing the Know-Your-Customer, anti-money laundering and payout functions in-house. Finance will be responsible for this with the assistance of the sales- and account management team.

As part of ensuring compliance with regulatory requirements, Slotmill will seek to carry out a verification of its customer's identity in two distinct functions; Know Your Customer (KYC) and continuing Customer Due Diligence (CDD). This process is based upon the risk-based methodology that is current best practice in anti-money laundering and compliance guidelines. Any suspicious transactions that are identified shall be reported to management where Finance has the overriding responsibility. Finance will investigate, analyze and if deemed necessary report the matter to the required regulatory body. All staff, contractors and consultants working for company will be made aware at the start of their employment or engagement about this policy. Any suspicious transfers must be reported by any staff member to both their immediate line manager and to Finance.

No staff member will need to seek permission to make a report and Finance will be obliged to record and investigate each and every report of potentially suspicious activity received.

Each month, Finance will be obliged to detail every report received and subsequently investigated to the CEO. Full disclosure of the nature of the report and all information found during the investigation will be made to the CEO. The CEO will consider the speed and depth with which investigations are made by Finance as key performance monitoring KPI for that role. Initial targets will be set as follows:

- Acknowledge receipt of report from staff member and explain the forthcoming procedure for investigation – 24 hours.
- Begin initial investigation and gather information regarding the suspicious transfer – 96 hours.
- If initial investigation finds a genuine high-risk transfer report to the Board – 24 hours of recognizing problem.
- Take action to remedy problem and inform authorities – 24 hours of making decision to take remedial action.

2.1 *Know Your Client (KYC) and Anti Money Laundering (AML)*

Slotmill has implemented a risk-based approach due diligence process, this includes any new client that is not been already vetted by Slotmill or by its licensing authority (MGA) moreover Slotmill reserves at all times, the right to conduct due diligence verifications. The purpose of having due diligence verifications on clients is to ensure that Slotmill has adequate mechanisms in place to determine who the client is, who is/are the beneficial owner/s, to determine whether such party is acting on behalf of another person, to establish the purpose and intended nature of the business relationship/occasional transaction and to monitor each business relationship on an ongoing basis.

In the case of business partners and clients, it will required them to provide the documents and information specified in Slotmill's due diligence Form, which includes but it is not limited to:

information about- and confirmation that the client hold a valid gambling licence(s), list of shareholders and directors, and confirmation that the party does not offer services to underage individuals or in restricted territories, as defined by Slotmill from time to time.

The due diligence procedures assist Slotmill in determining whether a client falls within its risk parameters and to understand the business profile of the client with sufficient clarity in order to identify those transactions that fall outside this profile and thus to be able to form an opinion which would be relevant for anti-money laundering (AML) purposes and identify suspicious transactions when necessary.

The CEO and any manager involved in signing new clients have a duty to inform Finance and to perform due diligence checks and verifications when deemed necessary. Verifications take place by making reference to documents, data or information obtained by the client or from a reliable and independent source. For the purposes of this obligation, a reliable and independent source includes, inter alia, credit rating agency, government authorities, departments or agencies.

3 Risk Assessment - Procedure

It is imperative to identify, product/service risk, interface risk and geographical risk. Please see Slotmills Risk Management Policy for additional information.

3.1 Product / Service Risk

Slotmill must exercise caution to products and services that are inherently more risky than others and a likelier channel for criminal activity.

3.2 Interface Risk

Interface risk is considered to be medium given that in a remote gaming environment, we do not interact with clients on a face-to-face basis, however we do make an effort to monitor player activities of any risk to us or the operator's business. If any suspicious player activity is detected, this is reported to the operator's risk and fraud team.

3.3 Geographical Risk

The geographical risk is the risk posed to us by the geographical location of the player and the source of wealth/funds of the business relationship. As Slotmill does not handle any player funds this risk is borne to the operator, and Slotmill shall to the extent possible ensure that operators follow the general direction governed by the FATF.

The FATF lists a number of factors that should be assessed in determining when a country poses a higher risk. These include:

- Countries subject to sanctions, embargoes or similar measures issued by international organizations such as the United Nations Security Council. In addition, in some circumstances, countries subject to sanctions or measures which may not be universally recognized may be given credence by Slotmill because of the standing of the issue and the nature of the measures;
- Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measures;
- Countries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organizations operating within them;
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

3.4 Risk Management Procedures

If it is suspected that a player pose a risk, this shall immediately be reported to the operator concerned providing all the possible evidence.

3.5 Tipping Off

- No one is to inform the player that a suspicious transaction has been reported, let alone divulge details of such transaction (not even to other members of staff).
- There are severe penalties under the Money Laundering Regulations for anyone who is found guilty of divulging such information.
- At no time should anyone indicate to third parties that a particular transaction has been reported as a suspicious one or that information has been requested by the Police on a particular transaction whether or not such transaction was reported as a suspicious one.

3.6 Reporting Procedures and Obligations

Slotmill will maintain adequate internal reporting procedures and the responsibility for this rest with Finance to whom knowledge or suspicion of money laundering and /or funding of terrorism shall be reported.

Where a subject person knows, suspects or has reasonable grounds to suspect that funds are the proceeds of criminal activity, that a transaction may be related to money laundering or the funding of terrorism, or that a person may have been, is or may be connected with money laundering or the funding of terrorism, or that money laundering or the funding of terrorism has been, is being or may be committed or attempted, that subject person shall, as soon as is reasonably practicable, but not later than five working days from when the knowledge or suspicion first arose, disclose that information, supported by the relevant identification and other documentation, to Finance.

3.6.1 Selection of new employees

Managers and any Employee in charge of recruitment and hiring independent contractors and/or consultants, shall ensure to have concluded the appropriate due diligence checks, including but not limited to verifying the candidate is not under the age of 18, obtaining professional references, confirming employment history and qualifications and provide a police conduct report any other supporting documents as required by Slotmill in accordance with the applicable law and regulation. This requirement must be applied whenever hiring take place irrespective of the position of the employee or the consultant / contractor.

3.6.2 Awareness and Training to Employees

All Employees are required to abide by the applicable law and regulation and Slotmill's Information Security Policy which are applicable to their specific role, and any guidelines issued by their Manager and/or Slotmill's CEO.

All employees are required to complete EU B2B Responsible Gambling training which is provide by an external consultant.

Slotmill will provide, either directly or through third parties, training to help Employees to identify the key obligations pertaining to their corresponding job duties in accordance with the laws and regulations applicable from time to time to Slotmill and online gaming industry's best practices.

4 Responsibility

Finance has overall responsibility for the effective operation of this policy and ensuring that it is updated regularly, but the day-to-day responsibility for overseeing its implementation may be delegated. All managers have a specific responsibility to operate within the boundaries of this policy, take effective steps so that all employees understand the standards of behavior expected of them, and to take action when behavior falls below its requirements.