Flutter™

Anti-Money Laundering & Countering Financing of Terrorism Policy

Applicability: Global

Issuing function: Legal & Commercial

A message from Pádraig Ó Riordain, Chief Legal Officer & Group Commercial Director

"Building a culture where we operate responsibly, honestly, fairly and in accordance with the laws in each of the jurisdictions in which we operate is essential to us at Flutter. It is the responsibility of everyone at every level to help build and maintain this culture by being aware of, and understanding the Money Laundering and Financing of Terrorism risks which face our business. This responsibility includes adhering to the requirements set out in this Policy. Thank you for taking the time to read and understand this Policy and for helping Flutter build and maintain a culture we can all be proud of."

I. Introduction, Purpose and Scope

Flutter Entertainment plc, and all of its subsidiaries ("Flutter"), is committed to conducting business honestly, fairly, and with respect for people in accordance with the law in each of the jurisdictions in which it operates.

This Policy applies to Flutter employees as well as board members, agency workers, volunteers, independent contractors and third parties working on behalf of the company (hereinafter to be referred to as "you").

This Policy has been approved by the Board Risk and Sustainability Committee (BRSC) or it's designate. It will be reviewed and updated on an annual basis and, if necessary, more frequently where regulations/business changes require it.

The purpose of this Policy is to outline:

i. What Money Laundering and Terrorist Financing are;
ii. Our approach to managing Money Laundering and Financing of Terrorism risks throughout our business;
iii. What your responsibilities are to guiding against Money Laundering and Financing of Terrorism risks; and
iv. The steps we all must follow when a possible or actual policy violation occurs.

This Policy is supported by the supplementary documentation outlined in section VI.

II. Statement of Policy

Key definitions

- Money Laundering : The process by which the proceeds of crime are concealed to disguise their illegal origin.
- Terrorist Financing: The provision, collection, or receipt of funds with the intent or knowledge that the funds will be used to carry out an act of terrorism.

Our approach to AML & CFT

Flutter is committed to complying with all AML and CFT laws and regulations in the jurisdictions in which it operates, by preventing the use of our products or systems to launder criminal proceeds, to finance terrorism, to evade taxation, or to bypass applicable AML & CFT laws. We reserve the right to suspend any customer or third-party relationship that is deemed contrary to relevant law. To help ensure that we do business in a compliant manner, we have implemented the following:

- Policies, standards, and training to ensure our colleagues understand what AML & CFT are, and what our roles and responsibilities are;
- Formal escalation channels to flag suspicions of possible or actual AML & CFT violations; and
- Frameworks and procedures designed to continuously monitor for AML & CFT risks in our global operations.

Summary of Flutter's AML & CFT standards

This Policy is supported by standards. The standards seek to establish a benchmark that is met consistently across all subsidiaries. Flutter's AML & CFT standards define (non-exhaustively):

- Governance and oversight
- Training and awareness
- Annual AML & CFT business risk assessments
- Customer due diligence
- Employee due diligence
- Third party due diligence
- Exiting customer and third-party relationships
- Internal and external reporting
- Record-keeping
- Independent program reviews, as applicable

Common red flags that you should look out for:

Sometimes, individuals and third parties will try and conceal their true identify or avoid the controls we have in place to detect and prevent Money Laundering or Financing of Terrorism. You must look out for, and report any red flags you come across in line with your local AML & CFT procedures and escalation channels including:

- At account opening, a player provides information that is misleading, vague, difficult to verify, in an attempt to conceal their true identify or evade our onboarding procedures
- A player appears to be depositing multiple transactions below the reporting threshold within a short period
- Transactional activity that is inconsistent with the player's apparent financial standing, their usual pattern of activities or occupational information
- Large and/or rapid movement of funds not aligned to usual playing behaviours

Issued by: Group Financial Crime
Highest approval authority: BRSC
Approval date: 13.12.2022

Version: 2.1
Information classification scale: Public
Document ID: FLU – CLO– COMP - ENG

- Transactions involving players identified by media and/or sanctions lists as being linked to a terrorist organisation or terrorist activities
- Open search sources show a player supports violent extremism or radicalisation
- A player who refuses to identify a source for funds or provides information that is false, misleading, or substantially incorrect

Local Financial Crime teams must ensure a Suspicious Activity/Transaction Report (SAR/STR) is sent to the relevant Competent Authority as required.

III. Roles and Responsibilities

We ask that:

You familiarise yourself with the content of this Policy and report any breach or wrongdoing (past, present, or likely future).
For Flutter employees,

- If you are acting in a supervisory position, ensure your team members are aware of this Policy and their obligations to identify and escalate red flags where appropriate
- When in doubt, seek guidance from your line manager or local Financial Crime team
- As a general rule, you should follow guidance from our Procurement and Compliance teams when engaging a third party to ensure appropriate background checks are completed

You should be aware that failure to comply with this Policy could result in disciplinary action up to, and including, termination of employment or a business relationship, if deemed appropriate by Compliance, HR or relevant line management.

IV. Reporting Policy Violations

You should raise any concern with someone who can help address them properly, depending on the circumstances, you may choose to report internally or externally via our Independent Confidential Reporting Service.

Internally

Your local Financial Crime team will be in the best position to address concerns over potential breaches of this Policy. You can also reach out to your line manager, Procurement team, or other trusted persons such as Flutter's own Legal Counsel or Internal Audit.

Externally

Where it is not possible or comfortable for you to raise a concern internally, or where a concern continues to be unresolved following consultation, you can and should submit a report through our Independent Confidential Reporting Service. Please refer to our Whistleblowing policy for details.

V. Relevant Contact Details

In the event of any questions with regards to the content, context or meaning of this document please contact:

Responsibility	Point of Contact	Email
Group Compliance	Group Head of Financial Crime	complianceenquires@flutter.com

VI. Supplementary Documentation

- Flutter Code of Ethics
- Flutter Sanctions Policy
- Flutter Anti-Bribery and Corruption Policy
- Flutter Gifts and Hospitality Policy
- Flutter Whistleblowing Policy

For Flutter employees, please refer to your local intranet for more information and access to supportive material