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. The purpose of this Policy is to outline:

I. What Money Laundering and Terrorist Financing are;
II. Our approach to Anti-Money Laundering and Countering Financing of Terrorism ("AML & CFT") 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 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 is supported by the supplementary documentation outlined in section VI.

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

II. Statement of Policy

Key Definitions

- **Money Laundering**: The process by which the proceeds of crime are concealed to disguise their illegal origin.
- **Financing of Terrorism**: The provision, collection, or receipt of funds with the intent or knowledge that the funds will be used for terrorist purposes.

Our Approach:

Flutter is committed to complying with all AML & 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 laws. To help ensure that we do business in a compliant manner, we have implemented the following:

- Policies, standards, and training to ensure understanding of roles and responsibilities;
- 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 our AML & CFT Policy Standards:

This Policy is supported by standards. The standards seek to establish a benchmark that is met consistently across all subsidiaries. AML &CFT areas of requirements (non-exhaustively) include:

Tone from the top	IT system requirements
Governance and oversight	Third party due diligence
Training and awareness	Exiting relationships [1]
Business risk assessments	Internal and external reporting
Customer due diligence	Record-keeping
Employee due diligence	Independent program reviews

Common Red Flags that You Should Look Out For:

Sometimes, individuals and companies will try to conceal their true identity 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 but not limited to:

- At onboarding or account opening, information provided is misleading, vague, difficult to verify, in an attempt to conceal their true identity or evade our onboarding procedures.
- Refusal to provide source for funds or information that is requested as part of the due diligence process.
- Multiple transactions deposited below the reporting threshold within a short period.
- Transactional activity that is inconsistent with their apparent financial standing, their usual pattern of activities or occupational information.
- Large and/or rapid movement of funds not aligned to usual behaviours.
- Transactions involving individuals or companies linked to a terrorist organisation or terrorist activities.
- Open search sources suggest support of violent extremism or radicalisation.

Local Financial Crime teams must ensure a Suspicious Activity Report (SAR) is sent to the appropriate regulatory body as required.

[1] Customer and Third Parties

Issued by: Group Financial Crime
Highest approval authority: BRSC
Approval date: 13/Dec/2023

Version: 2.0
Information classification scale: Public
Document ID: Flutter AML Policy - ENG

Flutter™

Anti-Money Laundering & Countering Financing of Terrorism Policy

Applicability: Global

Issuing function: Legal & Commercial

III. Roles and Responsibilities

Employees Must:

- Familiarise yourself with the content of this Policy;
- Ensure you complete the relevant training within the time frames allocated;
- Follow guidance from our Procurement, Human Resource, and Financial Crime teams when engaging a customer, employee or third party to ensure appropriate due diligence is completed;
- Understand your obligations to identify and escalate red flags or escalate where you are unclear;
- Report any breach or wrongdoing (past, present, or likely future);
- When in doubt, seek guidance from your line manager and local Financial Crime team.

Flutter Management Must:

- Communicate this Policy to your team to ensure awareness;
- Ensure your team understand their obligations to identify and escalate red flags where appropriate;
- Ensure your team have access to and are assigned all relevant trainings;
- Monitor compliance within your team to ensure training is completed in the allocated time frame;
- Report any breach or wrongdoing (past, present, or likely future).

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. Monitoring, Assurance and Breach Reporting

Compliance with this Policy is monitored and assurance activities are performed at regular intervals. You should raise any concern with someone who can help address them properly, namely your Financial Crime team. Depending on the circumstances, you may choose to report internally or externally via our Independent Confidential Reporting Service.

You should raise any concern with someone who can help address them properly. Your Compliance team may be in the best position to address concerns over potential breaches of this policy. You can also reach out on this matter to your line manager or other trusted persons such as Flutter's own Legal Counsel or Internal Audit. Where it is not possible or desirable to address a particular concern in consultation with your line manager, or where a reportable matter continues to be unresolved following consultation, you should submit a report about a reportable matter through the Speak-Up platform. 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 Financial Crime	The Financial Crime Team	GroupFinancialCrime@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
- Conflict of Interest Policy

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

Issued by: Group Financial Crime
Highest approval authority: BRSC
Approval date: 13/Dec/2023

Version: 2.0
Information classification scale: Public
Document ID: Flutter AML Policy - ENG