Flutter™

Third Party Financial Crime Policy

Applicability: Global

Issuing function: Legal & Commercial

A message from Flutter Chief Legal Officer

"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 Financial Crime 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 laws in each of the jurisdictions in which it operates. The purpose of this Policy is to outline:

i. The Group's Third Party Financial Crime (TPFC) risk position;
ii. Our approach to TPFC risk management throughout our business;
iii. What your responsibilities are to guiding against Third Party Financial Crime 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

Third Party: Any individual, or non-Flutter entity, including any directors or beneficial owners of such non-Flutter entity, which provides service(s) or good(s) to the Group and or, any non-Flutter entity who is or will be in receipt of Group funds or assets, this includes contractors, sub-contractors, Charities and Political Organisations.

Financial Crime: A broad term used to describe criminal activities that involve money, or other financial resources. It refers to any illegal activity that involves the use of financial systems, institutions, or instruments for illicit purposes, typically with the goal of generating profits for the perpetrators including, but not limited to, Money Laundering, Financing of Terrorism, Bribery and Corruption and Sanctions evasion.

Our approach to Third Party Financial Crime Risk

As a business with global Third Party relationships and high standards of corporate integrity, it is imperative that we protect our business reputation and secure ongoing compliance with international regulatory standards of conduct by ensuring that Third Parties with whom we contract, partner, engage or otherwise have a relationship with do not pose a significant Financial Crime related risk. 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;
- Robust Due Diligence processes;
- Formal escalation channels to flag suspicions; and
- Frameworks and procedures designed to continuously monitor for Financial Crime risks in our global operations.

Summary of our TPFC Policy Standards

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

Tone from the top	Contractual requirements
Governance and oversight	Record keeping
Standard and enhanced due diligence	Incident reporting
Ongoing Third Party risk management	Payment/release of funds
Business risk assessment	Training and awareness
Independent program review	Prohibited relationships
Jurisdictional risk	Third party red flags

Prohibited Relationships that You Should Look Out For

Sometimes, an individual or company will try to conceal their identity or avoid the controls we have in place to detect and prevent Financial Crime. You must look out for, and report any red flags you come across in line with your local AML & CFT, ABC and Sanctions standards, procedures and escalation channels including but not limited to a Third Party who:

- insist on anonymity when transacting with the Group;
- refuse to comply with Flutter's onboarding requirements;
- appear to be a Shell Company;
- appear on a Sanction list or are located in a prohibited jurisdiction;
- be convicted or suspected of terrorist financing; or
- associated with the arms trade/drugs.

Material Incidents related to Third Parties must be immediately communicated to the Chief Legal Officer & Group Commercial Director and Group Director of Compliance.

Issued by: Group Financial Crime
Highest approval authority: RSC
Approval date: 10 Dec 2024

Version: 1.0
Information classification scale: Public
Document ID: Flutter-TPFC -Policy - ENG

III. Roles and Responsibilities

Employees Must:

- Familiarise yourself with the content of this Policy;
- Ensure you complete relevant training within the time frames allocated;
- Follow guidance from our Procurement, Legal, Information Security, Tax and Financial Crime teams when engaging a 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 (past or present) and any wrongdoing that there is suspicion will lead to a breach in the 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 relevant policy standards and procedures;
- Monitor compliance within your team to ensure training is completed in the allocated time frame;

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

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 to your line manager or other trusted persons such as the Legal or Internal Audit teams. Where it is not possible or desirable to address a particular concern with your line manager, or where a reportable matter continues to be unresolved, you should submit a report 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	Name	Email
General queries and escalations related to Financial Crime	Group Financial Crime Team	GroupFinancialCrime@flutter.com

VI. Supplementary Documentation

- Flutter AML & CFT Policy.
- Flutter Anti-Bribery and Corruption Policy.
- Flutter Sanctions Policy.
- Flutter Code of Ethics.
- Flutter Gifts and Hospitality Policy.
- Flutter Conflict of Interest Policy.
- Flutter Whistleblower Policy.
- Flutter Procurement and Supplier Risk & Performance Management Policy.

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