



KYC / AML Policy

Effective: August 3, 2026 · **Version:** 1.0 · **Document Code:** FLG-CMP-001

Purpose & Regulatory Mandate

GOFUNDMEAFRICA LTD, operating the FlutterGive crowdfunding platform, enforces Know Your Customer (KYC) and Anti-Money Laundering (AML) controls to prevent fraud, identity theft, financial crime, and terrorist financing. These controls are designed to comply with the Money Laundering (Prevention and Prohibition) Act 2022, the Terrorism (Prevention and Prohibition) Act 2022, the Nigeria Data Protection Act 2023, and international standards including the FATF Recommendations.

Compliance Notice: All payouts are routed through licensed merchant account channels (Flutterwave — primary, live; Paystack — secondary adapter in development) and screened against global sanctions and Politically Exposed Person (PEP) databases before authorisation.

When Verification is Required

While campaign creation and receiving contributions are open immediately, full KYC verification is mandatory before processing any withdrawal or fund disbursement. Once a campaign receives its initial donation, automated compliance prompts activate within the organizer dashboard.

No funds may be disbursed to any organizer — individual or organisation — until their KYC has been reviewed and approved by our compliance team.

Required Documentation

Verification requirements differ for individuals and registered organisations:

Document	Requirement
Government ID	Valid Passport, National Identity Card, or Driver's License (unexpired)

Document	Requirement
Proof of Residence	Recent utility bill, bank statement, or tax document issued within the last 90 days
Live Selfie Verification	Live selfie captured via in-app camera. Submitted for automated liveness detection and 1:1 face-match verification against the ID document, followed by manual review

Registered NGO, corporate, and social enterprise accounts must additionally provide legal incorporation certificates, tax identification, and Ultimate Beneficial Owner (UBO) details.

Verification Method: FlutterGive uses a hybrid verification approach. Automated third-party screening (via Didit — identity document analysis, passive liveness detection, 1:1 face match, and device/IP analysis) produces a preliminary verdict and score. All submissions are then reviewed by a trained compliance officer who makes the final approval or rejection decision based on the aggregated automated results and any manual review notes. This hybrid model combines the speed and consistency of automation with the judgement of a human reviewer.

Payout Destination Matching

To prevent illicit diversion, the payout destination (bank account or mobile money wallet) linked for disbursement must strictly match the verified legal name on the campaign organizer's KYC profile. Third-party payouts and disbursements to unverified names are prohibited and will be blocked by our compliance review process.

Sanctions & PEP Screening

Before any payout is authorised, campaign organizers and payout beneficiaries are screened against:

- Global sanctions lists (OFAC, UN, EU, UK HMT, and applicable national lists).
- Politically Exposed Person (PEP) databases.
- Adverse media sources where applicable.

Screening combines automated system checks and manual review by our compliance team. Where a potential match is identified, the account is flagged, payouts are suspended, and the matter is escalated for further investigation.

Country Risk Assessment (FATF Lists)

FlutterGive maintains an internal reference of countries currently listed by the Financial Action Task Force (FATF) as subject to either a Call for Action (the FATF "Black List") or Increased Monitoring (the FATF "Grey List"). This reference is updated when FATF publishes amendments, approximately three times per year.

When an administrator reviews a payout request, the associated country risk information is displayed alongside the review. This supports our compliance team in applying a risk-based approach to payouts, in line with FATF Recommendation 10 (Customer Due Diligence) and Recommendation 19 (Higher-Risk Countries).

FlutterGive does not automatically deny service, donations, campaign creation, or KYC submission on the basis of country risk. Enhanced review is applied at the discretion of our compliance team where warranted by other risk factors.

Device & IP Reputation Screening

FlutterGive performs automated reputation checks on IP addresses at account signup and login. These checks are conducted using IPQualityScore (IPQS), a third-party fraud-prevention service, and are used exclusively for fraud detection, abuse prevention, and platform security purposes.

Reputation signals captured include a fraud score and whether the IP address is associated with a proxy, VPN, Tor exit node, bot activity, or recent abuse. Results are stored in our internal compliance systems and are not shared publicly.

Review process: A single VPN or proxy flag is common and is not treated as suspicious on its own. Higher-severity signals (Tor, bot activity, high fraud score, or recent abuse) trigger an internal review, during which our compliance team may:

- Cross-reference the flagged IP against other accounts and activity on the platform.
- Apply additional scrutiny to KYC documentation and payout destination matching.
- Log the review outcome in our moderation audit trail.

IP reputation signals are considered alongside other risk factors. They are not used in isolation to deny service, and they do not block signup, login, donations, or campaign creation.

Transaction Monitoring

FlutterGive maintains a layered transaction monitoring framework to detect anomalous tipping, micro-donation abuse, velocity anomalies, structured payments, and coordinated money-laundering schemes:

- Automated transaction velocity limits and IP-based rate limiting.
- Micro-donation risk scoring and donation pattern analysis.
- Automated withdrawal holds upon community reports (three or more distinct-source reports within 24 hours).
- Manual moderation review prior to settlement clearing.
- Complete audit trail of admin actions, moderation decisions, and system events.
- Login monitoring, failed-login alerts, and account lockout controls.

Suspicious Activity Handling

Where transactions or account activity are flagged as suspicious:

- The account and any linked campaign payouts are frozen immediately.
- All related transaction records, KYC documentation, and audit logs are preserved.
- The matter is escalated to the compliance team for investigation.
- Where warranted, a Suspicious Activity Report (SAR) is filed with the relevant Financial Intelligence Unit (FIU) — including the Nigerian Financial Intelligence Unit (NFIU) for Nigerian operations.
- The affected user is notified in accordance with applicable law.

Record Retention

In compliance with the Money Laundering (Prevention and Prohibition) Act 2022 and FATF Recommendation 11, FlutterGive retains all KYC documents, transaction records, sanctions screening results, and audit logs for a minimum of **five (5) years** from the date of the last transaction or account closure. Records are stored securely, encrypted where applicable, and available to regulators and law enforcement upon lawful request. This retention also aligns with the Nigeria Data Protection Act 2023.

Regulatory Reporting

FlutterGive cooperates fully with financial intelligence units, central banks, and law enforcement agencies in any jurisdiction where it operates. Where required by law, suspicious activity, sanctions matches, and criminal conduct are reported to the appropriate authority without prior notice to the affected user. We also cooperate with requests from our licensed payment partners (Flutterwave and Paystack) in relation to transaction monitoring and regulatory compliance.

Contact

For questions regarding identity verification, document re-submission, or compliance procedures, contact our compliance team at legal@fluttergive.com.