Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Policy

For Finova Global Technologies

---

1. Policy Statement

Finova Global Technologies LTD is fully committed to complying with the Anti-Money Laundering Act, 2020 (Act 1044), the Anti-Terrorism Act, 2008 (Act 762), and directives issued by the **Bank of Ghana**, **Securities and Exchange Commission**, and the **Financial Intelligence Centre (FIC)**.

As a mobile-first services provider using USSD technology, mobile app, and web app, we recognize the importance of safeguarding its platform against the risks of money laundering (ML), terrorist financing (TF), and other illicit financial activities.

This policy aims to:

- Prevent, detect, and report suspicious activities
- Apply risk-based Know Your Customer (KYC) and Customer Due Diligence (CDD) procedures
- Implement robust transaction monitoring and internal reporting frameworks
- Maintain strong data protection and record-keeping practices
- Promote a culture of compliance through staff training and accountability

---

2. Legal and Regulatory References

Our AML/CTF framework is guided by the following Ghanaian laws and directives:

- **Anti-Money Laundering Act, 2020 (Act 1044)**
- **Anti-Terrorism Act, 2008 (Act 762)**
- **FIC Guidelines for Designated Non-Financial Businesses and Professions (DNFBPs)**
- **BoG AML/CFT & Sanctions Compliance Guidelines (2021)**
- **SEC Guidelines on AML/CFT for Capital Market Operators**
- **FIC Directive on Suspicious Transaction Reporting (STR)**

---

3. Definitions (Ghana Context)

Term	Definition
Money Laundering (ML)	Concealing the source of illicit funds to make them appear legitimate.
Terrorist Financing (TF)	Providing or collecting funds with the intention of supporting terrorist acts.
Politically Exposed Person (PEP)	A person holding a prominent public function in Ghana or abroad.
Suspicious Transaction Report (STR)	Report submitted to the FIC when a transaction raises red flags.
Enhanced Due Diligence (EDD)	Heightened verification and scrutiny applied to high-risk individuals or activities.
FIC	Financial Intelligence Centre of Ghana – the national FIU.

---

4. Risk-Based Approach

Finova Global Technologies apply a **Risk-Based Approach (RBA)** as mandated by BoG and FIC to ensure that resources are allocated proportionally to identified risks. Risk assessments are updated **annually**.

Key Risk Categories:

- **Customer Risk**: anonymous or unverifiable users, PEPs, and non-residents
- **Channel Risk**: non-face-to-face onboarding through USSD
- **Geographic Risk**: high-risk or non-cooperative jurisdictions identified by the FIC or FATF
- **Product Risk**: mobile-based fund transfers with limited documentation

Risk Mitigation Measures:

- Tiered transaction limits
- SIM registration validation via telco APIs
- Real-time transaction monitoring and anomaly detection
- Manual and automated screening of all users

---

5. Customer Due Diligence (CDD)

5.1 Individual Users

All users must provide:

- Full name
- Date of birth
- Nationality
- Government-issued ID (Ghana Card, Passport, or Driver's License)
- SIM-registered phone number
- Proof of address (optional for low-risk accounts)

5.2 Business Users (Where Applicable)

- Certificate of incorporation (Registrar General's Department)
- Company TIN
- Names and IDs of directors and beneficial owners (≥10%)
- Business address and license (if applicable)

5.3 Enhanced Due Diligence (EDD)

EDD is applied in cases involving:

- PEPs or their associates
- Transactions exceeding GHS 10,000
- Users flagged in internal monitoring or sanctions screening
  EDD measures include:
- Source of funds and wealth declarations
- Senior compliance approval
- Ongoing review of transaction activity

---

6. Transaction Monitoring & Reporting

6.1 Monitoring

All transactions across our applications are:

- Logged in real-time
- Flagged when anomalies are detected (e.g., repeated small transactions near limit, geographic mismatches)
- Subject to batch reviews for patterns consistent with money laundering or structuring

6.2 Reporting

- **Suspicious Transaction Reports (STRs)** are filed directly with the **Financial Intelligence Centre (FIC)** via email account info@fic.gov.gh or such other address as may be notified from time to time.
- Reports must be submitted within **24 hours** of suspicion identification
- **Large Cash Transactions** (over GHS 10,000) will be reported as per BoG guidelines

6.3 Escalation Path

Operational Staff → Compliance Officer → Money Laundering Reporting Officer (MLRO) → FIC

---

7. Sanctions and PEP Screening

Finova Global Technologies will use automated systems to screen users against:

- OFAC Sanctions List
- Local watchlists from Ghana's Ministry of National Security or FIC
- PEP and adverse media databases

Screening is conducted:

- At onboarding
- Daily for active users
- Before processing high-risk transactions

---

8. Record Keeping & Data Protection

- All CDD documents, STRs, and transaction logs are stored securely for **a minimum of 5 years**, in accordance with Act 1044
- Data is encrypted and access is restricted based on staff roles

- Data protection practices are aligned with the **Ghana Data Protection Act, 2012 (Act 843)**

---

9. Staff Training & Whistleblower Protection

- **Mandatory AML/CFT training** for all employees during onboarding and annually
- **Refresher sessions** cover new threats, STR procedures, and regulatory changes
- **Whistleblower protections** align with Ghana's Whistleblower Act, 2006 (Act 720)
- Anonymous reporting is available via secure internal email or submission box

---

10. Internal Audit & Policy Review

- AML/CTF compliance is audited **annually** by an internal or independent auditor
- Policy is reviewed **every two years** or sooner upon major regulatory changes
- Audit findings are shared with senior leadership and used to enhance controls

---

11. USSD Platform Controls

To address the unique risks of mobile financial services:

Tier	Verification Level	Daily Limit
Tier 0	Unverified (Phone only)	GHS 0 (No transactions allowed)
Tier 1	Basic KYC (ID + SIM)	GHS 3,000
Tier 2	Full KYC	GHS 10,000+

Other USSD-specific security features:

- Session timeouts
- PIN and passkey authentication
- Activity time-limits to prevent SIM takeover

---

12. Policy Communication & Enforcement

- Policy distributed to all employees and contractors upon joining
- Acknowledgement of understanding is mandatory
- Violations may lead to disciplinary action, including termination and reporting to authorities

---

✅ Approval & Review

Approved by: Board of Directors – Finova Global Technologies LTD
Effective Date: [25/04/2025]
Next Review Date: [25/05/2027]