



Afriq Global Market Limited

Vendor Onboarding and KYC Policy

|

Version 2.0 (Final)

|

Effective 1 September 2026

CONFIDENTIAL — INTERNAL COMPLIANCE DOCUMENT

Document Title	Vendor Onboarding and KYC Policy
Version	2.0 (Final)
Previous Version	1.1 (Amendment — 5 August 2026) — Superseded and Replaced in Full
Effective Date	1 September 2026
Classification	CONFIDENTIAL — INTERNAL COMPLIANCE DOCUMENT
Jurisdiction	Multi-Jurisdictional: United States of America (Michigan); Federal Republic of Nigeria; United Kingdom; European Union; Canada; and other applicable African jurisdictions
Purpose	Know Your Customer, Know Your Business, and Anti-Money Laundering Compliance Framework
Issued By	Afriq Global Market Limited — Compliance and Operations
Related Documents	Privacy Policy v3.0; Service Agreement v4.0; Acceptable Use Policy
Website	www.afriqglobal.org
Review Cycle	Annual, or upon material regulatory change
Contact	davidsopekan@afriqglobal.org

AMENDMENT NOTICE — VERSION 2.0 — EFFECTIVE 1 SEPTEMBER 2026

This Policy Version 2.0 supersedes and replaces Version 1.1 (dated 5 August 2026) in its entirety.

Key changes from v1.1 to v2.0:

1. All internal numbering corrected throughout — all sub-items within each Section now start at 1 within that Section (v1.1 contained continuous list numbering across sections, which was a document formatting error);
2. Related documents updated: Privacy Policy v3.0; Service Agreement v4.0;
3. Effective date updated to 1 September 2026;

4. All South Africa references already removed in v1.1 — confirmed removed in full in v2.0;
5. PayPal fully removed (already removed in v1.1) — confirmed in v2.0;
6. Buyer verification section added (new Section 6A) — the Platform verifies buyers as well as vendors for fraud prevention and compliance purposes.

Table of Contents

Section 1	Introduction and Purpose
Section 2	Scope
Section 3	Definitions
Section 4	Vendor Eligibility
Section 5	Onboarding Process
Section 6	Identity Verification Requirements (Vendors)
Section 6A	Buyer Verification (<i>New — v2.0</i>)
Section 7	Business Registration Verification
Section 8	Bank and Payment Account Verification
Section 9	Document Requirements by Jurisdiction
Section 10	Vendor Categories and Risk-Based Approach
Section 11	Manual Review Process
Section 12	Risk Categorisation
Section 13	Ongoing Monitoring
Section 14	AML Compliance
Section 15	Data Retention
Section 16	Escalation and Dispute Resolution
Section 17	Governing Compliance Framework
Section 18	General Provisions

Section 1 — Introduction and Purpose

1.1 Afriq Global Market Limited ("Company", "Platform") operates a multi-vendor, business-to-consumer (B2C) e-commerce marketplace connecting African vendors with buyers across the world. The Platform processes cross-border payments and facilitates international commerce in multiple currencies across multiple jurisdictions.

1.2 This Vendor Onboarding and KYC Policy ("Policy") establishes the Company's framework for:

1. Verifying the identity of all vendors prior to and during their use of the Platform;
2. Verifying the registration and legitimacy of business vendors;
3. Conducting Anti-Money Laundering (AML) and sanctions compliance screening;
4. Assessing and managing the risk presented by individual vendors;
5. Conducting baseline verification of buyers to prevent fraud and platform abuse.

1.3 The objectives of this Policy are to:

6. Protect the Platform, its users, and the Company from fraud, money laundering, terrorist financing, and other financial crimes;
7. Ensure compliance with applicable Know Your Customer (KYC) and Know Your Business (KYB) regulations across all jurisdictions in which the Platform operates;
8. Maintain the trust of buyers, vendors, payment partners, and regulatory authorities;
9. Establish a clear and consistent onboarding standard for all Platform participants.

1.4 This Policy applies to all vendors registered or seeking registration on the Platform and to all buyer verification activities conducted by the Platform. This Policy must be read together with the Privacy Policy v3.0, the Service Agreement v4.0, and the Acceptable Use Policy.

Section 2 — Scope

2.1 This Policy applies to:

10. All individual vendors, sole traders, and business entities registered or applying to register as vendors on the Platform;
11. All buyers whose activity triggers enhanced verification under Section 6A;
12. All persons involved in onboarding, compliance review, and vendor management within the Company.

2.2 Geographic Scope. This Policy applies to vendors and buyers from the following jurisdictions:

13. United States of America (with particular reference to Michigan state law and federal financial regulations);
14. Federal Republic of Nigeria;
15. United Kingdom;
16. European Union member states;
17. Canada;
18. All other African jurisdictions from which vendors are onboarded or buyers transact.

2.3 The Company does not currently operate under a South African regulatory mandate. All references to the Republic of South Africa, POPIA, FICA, and the FIC have been removed from this Policy.

Section 3 — Definitions

Term	Definition
AML	Anti-Money Laundering — the body of laws, regulations, and procedures designed to prevent the generation of income through illegal activities.
Beneficial Owner	Any natural person who directly or indirectly owns or controls more than twenty-five percent (25%) of a vendor entity, or who otherwise exercises effective control over the vendor entity.
Biometric Verification	The use of liveness detection and facial comparison technology to confirm that a person submitting documents is physically present and matches the identity document provided.
Dojah	Dojah Inc., the Company's designated identity verification technology partner for Nigerian and African vendor KYC processing.
EFCC	The Economic and Financial Crimes Commission of Nigeria, established under the Economic and Financial Crimes Commission (Establishment) Act 2004.
Enhanced Due Diligence (EDD)	Additional verification measures applied to vendors assessed as presenting a higher risk of fraud, money laundering, or other financial crime.
Flutterwave	Flutterwave Technology Solutions Limited, the Company's payment processing partner for within-Africa transactions and supported international currency transactions.
KYB	Know Your Business — the process of verifying the legal existence, ownership structure, and regulatory standing of a business entity.
KYC	Know Your Customer — the process of verifying the identity of individual persons in accordance with applicable AML and financial crime prevention regulations.
MLPA	The Money Laundering Prohibition Act 2011 of Nigeria and any amendments thereto.
NDPA	The Nigerian Data Protection Act 2023.
NDPC	The Nigeria Data Protection Commission established under the NDPA.
OFAC	The United States Department of the Treasury's Office of Foreign Assets Control, which administers and enforces economic and trade sanctions.
Paystack	Paystack Payments Limited, the Company's payment processing partner for NGN and within-Africa transactions.
PEP	Politically Exposed Person — an individual who holds or has held a prominent public position or function, or who is a close associate or family member of such an individual.
Risk Assessment	The process of evaluating the level of financial crime risk presented by a vendor based on their identity, business type, jurisdiction, transaction patterns, and other relevant factors.

Term	Definition
Sanctions	The economic or financial sanctions lists maintained by OFAC, the United Nations Security Council, the European Union, the United Kingdom's His Majesty's Treasury, and other applicable regulatory authorities.
Smile Identity	Smile Identity Inc., the Company's designated identity verification technology partner for international, diaspora, and non-Nigerian vendor KYC processing.
Stripe	Stripe, Inc., the Company's payment processing partner for non-NGN international transactions.
Terminal Africa	Terminal Africa Limited, the Company's exclusive integrated logistics partner for local, intra-Africa, and international shipment services.
Vendor Dashboard	The administrative interface provided to verified vendors for managing listings, orders, payouts, and account settings.

Section 4 — Vendor Eligibility

To be eligible to register as a vendor on the Platform, an applicant must satisfy all of the following requirements:

4.1 Age. The applicant must be at least eighteen (18) years of age, or of the legal age of majority in their jurisdiction of residence (whichever is higher).

4.2 Identity. The applicant must hold a valid, unexpired, government-issued identity document as specified in Section 6.

4.3 Business Registration (where applicable). An applicant registering as a business entity must be a duly registered, legally constituted, and valid business entity in good standing under the laws of the applicable jurisdiction.

4.4 Payment Account. The applicant must hold a verified bank account or payment processing account (Paystack or Flutterwave for African vendors; Stripe or Flutterwave for international vendors) in their own name or in the registered name of their business entity.

4.5 No Sanctions. The applicant must not appear on any Sanctions list administered by OFAC, the UN Security Council, the European Union, the UK HM Treasury, or any other applicable regulatory authority.

4.6 No Prior Adverse History. The applicant must not have had a prior vendor account on the Platform terminated for fraud, AML violations, misrepresentation, or serious breach of the Service Agreement.

4.7 Lawful Products. The applicant must confirm that the Products they intend to sell on the Platform are lawful and do not fall within the categories set out in the Prohibited and Restricted Products Schedule (Appendix B to the Service Agreement v4.0).

4.8 Policy Acceptance. The applicant must read, understand, and formally accept the Service Agreement v4.0, this Policy, the Privacy Policy v3.0, and the Acceptable Use Policy.

Section 5 — Onboarding Process

The vendor onboarding process consists of the following sequential steps:

5.1 Step 1 — Account Creation. The applicant creates an account on the Platform by providing:

- 19. Full legal name;
- 20. Email address and mobile telephone number;
- 21. Jurisdiction of residence or business registration;
- 22. Intended product categories.

5.2 Step 2 — Identity Verification. The applicant completes identity verification through the Platform's integrated KYC provider:

- 23. Nigerian and African vendors: identity verification via Dojah, including government-issued ID upload and liveness check;
- 24. International and diaspora vendors: identity verification via Smile Identity, including document verification and biometric check.

The identity verification process is described in detail in Section 6.

5.3 Step 3 — Business Verification (Business Vendors Only). Applicants registering as a business entity (rather than as an individual) must complete business registration verification as described in Section 7.

5.4 Step 4 — Payment Account Linking. The applicant links their verified payment account:

- 25. Nigerian and African vendors: Paystack account (NGN) or Flutterwave account (supported African currencies);
- 26. International vendors: Stripe account or Flutterwave account (supported international currencies).

Payment account verification is described in detail in Section 8.

5.5 Step 5 — Sanctions and PEP Screening. The Company conducts automated sanctions and PEP screening against the applicant's verified identity details, using approved screening databases. Vendors who appear on a Sanctions list are automatically declined. Vendors identified as PEPs are subject to Enhanced Due Diligence (EDD) as described in Section 11.

5.6 Step 6 — Policy Acceptance. The applicant formally accepts the Service Agreement v4.0, this Policy, the Privacy Policy v3.0, and the Acceptable Use Policy through a recorded digital acceptance mechanism.

5.7 Step 7 — Account Activation. Upon successful completion of all preceding steps and approval by the compliance system (or, where required, by a compliance officer), the applicant's vendor account is activated and they gain access to the Vendor Dashboard.

Onboarding Steps Summary

Step	Stage	Description
1	Account Creation	Name, email, phone, jurisdiction, product categories
2	Identity Verification	KYC via Dojah (African) or Smile Identity (international)
3	Business Verification	Business vendors only — registration documents
4		

Payment Account Linking

Paystack / Flutterwave (African); Stripe / Flutterwave (international)

5

Sanctions & PEP Screening

Automated screening; PEPs referred to EDD

6

Policy Acceptance

Recorded digital acceptance of all Platform policies

7

Account Activation

Compliance approval and Vendor Dashboard access granted

Section 6 — Identity Verification Requirements (Vendors)

6.1 Government-Issued Identity Document. All vendor applicants must submit a clear, legible copy of one valid, unexpired government-issued photo identity document. Acceptable documents include:

27. International passport;

28. National identity card (where issued by the relevant national authority);

29. Driver's licence (where it includes a photograph and date of birth).

6.2 Liveness Check and Biometric Verification. All vendor applicants must complete a liveness check through the Platform's KYC provider (Dojah for Nigerian/African vendors; Smile Identity for international vendors). The liveness check involves:

30. A selfie or short video capture at the time of application;

31. Automated facial comparison between the live capture and the submitted identity document;

32. Liveness detection to confirm the submission is from a live person and not a photograph or recording.

6.3 Address Verification. Vendor applicants must provide their residential or business address. Address verification may be completed through one or more of the following:

33. A utility bill, bank statement, or official government correspondence dated within the last three (3) months;

34. An address confirmation provided through the KYC provider's integrated address verification service;

35. A notarised declaration of address (for applicants in jurisdictions where the above documents are not readily available).

6.4 Additional Documentation. The Company or its KYC providers may request additional documents where necessary to complete the verification process, including where:

36. The submitted documents are unclear, expired, or of insufficient quality;

37. The automated verification system raises a flag requiring manual review;

38. The Company's risk assessment process determines that enhanced verification is required.

Section 6A — Buyer Verification [New — Version 2.0]

Version 2.0 Addition

This Section is new in Version 2.0. It was not present in Version 1.1. It establishes the Platform's framework for buyer-side verification, conducted for fraud prevention and compliance purposes.

6A.1 Purpose. While the Platform's primary verification focus is on vendors, the Company also conducts baseline and, where necessary, enhanced verification of buyers to prevent fraud, money laundering, account takeover, and platform abuse.

6A.2 Baseline Buyer Verification. All buyers are required to:

39. Register on the Platform using a valid email address;

40. Verify their mobile telephone number via a one-time passcode (OTP);

41. Provide a valid delivery address when placing an order.

6A.3 Enhanced Buyer Verification Triggers. The Company's fraud prevention systems may trigger enhanced buyer verification in any of the following circumstances:

42. The buyer's transaction value in a single session exceeds a defined threshold;

43. The buyer's transaction pattern (including frequency, value, or destination) is flagged as unusual by the Platform's fraud detection system;

44. The buyer's payment method is associated with a previously flagged or blocked account;

45. The buyer's delivery address presents a high-risk profile;

46. A Payment Processor flags a transaction for additional verification.

6A.4 Enhanced Buyer Verification Process. Where enhanced verification is triggered, the buyer may be required to:

47. Provide a government-issued photo identity document;

48. Complete a liveness check;

49. Confirm payment account ownership.

Transactions subject to enhanced verification will be held pending completion of the verification process.

6A.5 Buyer Data. All personal data collected from buyers for the purposes of this Section is processed in accordance with the Privacy Policy v3.0.

Section 7 — Business Registration Verification

7.1 Certificate of Incorporation or Registration. Business vendors must provide a certified copy of their certificate of incorporation, certificate of registration, or equivalent constitutional document confirming the legal existence of the entity.

7.2 Business Address Verification. Business vendors must provide documentary evidence of their registered business address (utility bill, bank statement, or local government rate payment in the business name, dated within three (3) months).

7.3 Tax Identification. Business vendors must provide their Tax Identification Number (TIN) or equivalent tax registration reference as required in their jurisdiction. See Section 9 for jurisdiction-specific requirements.

7.4 Business Licence. Where the vendor's intended product categories require a specific trading or sector licence (for example, pharmaceutical distribution, food importation, or cosmetics), the business vendor must provide a valid copy of the relevant licence.

7.5 Directors and Beneficial Owners. Business vendors must disclose:

50. The full names, nationalities, and dates of birth of all directors or equivalent governing officers;

51. The full names, nationalities, and approximate ownership percentages of all Beneficial Owners (individuals holding more than 25% of shares or voting rights, or who otherwise exercise effective control).

Directors and Beneficial Owners are subject to individual identity verification under Section 6 and to sanctions and PEP screening under Section 5.5.

Section 8 — Bank and Payment Account Verification

8.1 Paystack (Nigerian and African Vendors). Nigerian and African vendors linking a Paystack account must verify that the Paystack account is registered in the same name as the verified vendor identity. The Company and Paystack's integrated APIs verify account ownership as part of the account linking process.

8.2 Flutterwave (African and International Vendors). Vendors using Flutterwave must verify their Flutterwave account through Flutterwave's standard identity verification process. Account ownership is confirmed by Flutterwave's KYC and financial compliance checks.

8.3 Stripe (International Vendors). Vendors using Stripe for international payouts must complete Stripe's standard identity and business verification process. The Stripe account must be in the same name as the verified vendor identity or business entity.

8.4 Account Mismatch. Where a payment account is in a different name from the verified vendor identity, the vendor must provide documentary evidence explaining the discrepancy (for example, a name change certificate or a corporate account authorisation letter). The compliance team will review such cases manually before activation.

8.5 Single Account Requirement. Vendors may link only one primary payout account at a time. Any change to the payout account must be verified through the re-verification process as described in Section 13.

Payment Partner Summary

Payment Partner

Applicable Vendors

Currency / Scope

Paystack

Nigerian and African vendors

NGN and within-Africa transactions

Flutterwave

African and international vendors

Supported African and international currencies

Stripe

International vendors

Non-NGN international transactions

Section 9 — Document Requirements by Jurisdiction

9.1 Nigeria

Requirement	Details
Government-Issued ID	National Identity Card (NIMC NIN), International Passport, or Driver's Licence

Requirement	Details
Business Registration	Corporate Affairs Commission (CAC) Certificate of Incorporation or Business Name Registration
Tax Identification	Federal Inland Revenue Service (FIRS) TIN
Additional	Bank Verification Number (BVN) for financial account verification; EFCC clearance where required by risk assessment

9.2 United States of America

Requirement	Details
Government-Issued ID	US Passport, State Driver's Licence, or State-Issued ID Card
Business Registration	State-level Certificate of Formation or Articles of Incorporation
Tax Identification	Social Security Number (SSN) for individuals; Employer Identification Number (EIN) for business entities
Additional	State business licence where required by product category or state law

9.3 United Kingdom

Requirement	Details
Government-Issued ID	UK Passport, UK Driver's Licence (with photograph), or UK Biometric Residence Permit
Business Registration	Companies House Certificate of Incorporation
Tax Identification	Unique Taxpayer Reference (UTR) and, where applicable, VAT Registration Number
Additional	FCA authorisation number where regulated financial activity is involved

9.4 European Union

Requirement	Details
Government-Issued ID	National Identity Card or EU Member State Passport

Requirement	Details
Business Registration	Relevant national commercial register extract (e.g., Handelsregister, KVK, INPI, RCS)
Tax Identification	National tax registration number and EU VAT number where applicable
Additional	Relevant sector licences where required by product category

9.5 Canada

Requirement	Details
Government-Issued ID	Canadian Passport, Provincial Driver's Licence, or Provincial ID Card
Business Registration	Federal or provincial Certificate of Incorporation or Business Registration
Tax Identification	Canada Revenue Agency Business Number (BN)
Additional	Provincial business licences as required

9.6 Other African Jurisdictions

Vendors from African jurisdictions not specifically listed above must provide:

- 52. A valid, unexpired, government-issued photo identity document from their country of residence;
- 53. Relevant business registration documentation issued by the applicable national authority;
- 54. Tax identification or equivalent as required by the laws of their jurisdiction;
- 55. Any additional documentation required by the Company's compliance team based on risk assessment.

Section 10 — Vendor Categories and Risk-Based Approach

10.1 Vendor Categories. The Company recognises the following categories of vendor, each subject to a proportionate level of verification:

Vendor Category	Description	Verification Requirements
Individual / Sole Trader	A natural person selling goods under their own name.	Government-issued ID; liveness check; address verification; payment account verification; sanctions/PEP screening.
Registered Business	A company, partnership, or registered legal entity.	All individual requirements above plus: certificate of incorporation/registration; business address verification; tax ID; director and beneficial owner identification; business-level sanctions and PEP screening.
Manufacturer	A business entity that produces goods it sells directly on the Platform.	All registered business requirements above plus: product registration or certification documentation (e.g., NAFDAC registration in Nigeria); proof of manufacturing facility or production licence.
Distributor / Wholesaler	A business entity sourcing goods from multiple manufacturers or suppliers for resale through the Platform.	All registered business requirements above plus: supplier agreements or procurement documentation to establish legitimate provenance; any applicable import or trading licences.

10.2 Risk-Based Verification Scaling. The Company applies a risk-based approach to verification, proportionate to the level of risk presented by the vendor category, jurisdiction, product type, and expected transaction volume. Higher-risk vendors receive Enhanced Due Diligence (EDD) as described in Section 11.

Section 11 — Manual Review Process

11.1 When Manual Review is Triggered. A vendor application will be referred for manual review by a compliance officer in any of the following circumstances:

- 56. Automated identity verification fails to confirm a match above the required confidence threshold;
- 57. The vendor is identified as a PEP or as a close associate of a PEP;
- 58. The vendor operates in a high-risk product category;
- 59. The vendor is registered in a jurisdiction assessed as presenting elevated AML/financial crime risk;
- 60. Inconsistencies are identified in the documents submitted;

61. The vendor's transaction profile in a previously held account raised concerns.

11.2 Manual Review Process.

62. The compliance officer will review all documents and system flags within five (5) business days of referral;

63. Where additional documents or information are required, the vendor will be notified via email with a specific list of required documents and a deadline for submission (minimum ten (10) business days);

64. The compliance officer may escalate cases to the Company's senior compliance function where the risk assessment cannot be resolved at first review level;

65. A final decision (approved, approved with conditions, or declined) will be communicated to the vendor applicant in writing within fifteen (15) business days of all required documents being received.

11.3 Enhanced Due Diligence (EDD). Where a vendor is approved following EDD, the Company may impose conditions including:

66. Enhanced transaction monitoring;

67. Restrictions on product categories or maximum order values;

68. More frequent periodic re-verification;

69. Escalated review of payout requests.

Section 12 — Risk Categorisation

12.1 All vendors are assigned a risk category upon onboarding and are reassessed periodically or when a triggering event occurs.

Risk Category	Criteria	Consequence
LOW RISK	Identity and business registration fully verified with high-confidence automated results; no sanctions or PEP matches; vendor's product category and jurisdiction	Standard onboarding and monitoring. Re-verification every 24 months.

Risk Category	Criteria	Consequence
	present no elevated risk flags; clean account and transaction history.	
MEDIUM RISK	Minor identity verification flags resolved through manual review; vendor newly established (under 6 months); documentation incomplete at application but later supplemented; product category on elevated-scrutiny list; jurisdiction on FATF grey-list or equivalent.	Additional document requirements; closer initial monitoring; re-verification every 12 months.
HIGH RISK	Vendor identified as a PEP or closely associated with a PEP; registered in FATF high-risk or non-cooperative jurisdiction; prior compliance flags recorded; transaction patterns raise AML or fraud concerns; conflicting information across submitted documents.	EDD required; restricted platform access until EDD complete; ongoing enhanced monitoring; re-verification every 6 months or as directed.

Section 13 — Ongoing Monitoring

13.1 Periodic Re-Verification. All vendors are subject to periodic re-verification at the following intervals:

- 70. Low Risk vendors: every twenty-four (24) months;
- 71. Medium Risk vendors: every twelve (12) months;
- 72. High Risk vendors: every six (6) months or as directed by the compliance function.

13.2 Triggering Events. In addition to scheduled re-verification, immediate re-verification is triggered by:

- 73. A change in the vendor's name, business registration details, or payment account;
- 74. A significant and unexplained change in transaction volume or pattern;
- 75. A customer complaint or dispute raising identity or fraud concerns;
- 76. A sanctions or PEP alert generated by the monitoring system;
- 77. Regulatory direction or legal process.

13.3 Transaction Monitoring. The Platform applies automated transaction monitoring tools to detect patterns associated with fraud, money laundering, or platform policy abuse, including:

- 78. Unusually high transaction volumes for a given vendor category;
- 79. Transactions inconsistent with the vendor's stated business purpose;

80. Multiple orders from the same IP address or device fingerprint across different buyer accounts;

81. Rapid cycling of funds through the Platform without apparent commercial purpose.

13.4 Compliance Holds. Where transaction monitoring identifies a concern, the compliance team may place a temporary hold on the relevant vendor's payouts while the concern is investigated. The vendor will be notified of the hold within two (2) business days. The Company will investigate and reach a determination within fifteen (15) business days of the hold being placed.

Section 14 — AML Compliance

14.1 Sanctions Screening. All vendors, directors, and beneficial owners are screened against the following sanctions lists at onboarding and at each periodic re-verification:

82. OFAC Specially Designated Nationals and Blocked Persons List (SDN);

83. United Nations Security Council Consolidated Sanctions List;

84. European Union Consolidated Financial Sanctions List;

85. United Kingdom HM Treasury Consolidated List of Financial Sanctions Targets;

86. Any other applicable national or international sanctions list.

14.2 PEP Screening. All vendors, directors, and beneficial owners are screened for PEP status at onboarding and periodically thereafter. PEP identification does not automatically result in declination; however, PEPs are subject to Enhanced Due Diligence (EDD) and senior management approval before account activation.

14.3 Suspicious Activity Reporting. Where the Company identifies activity that gives rise to a reasonable suspicion of money laundering, terrorist financing, or other financial crime, it is obligated to file a Suspicious Activity Report (SAR) or equivalent report with the relevant authorities in the applicable jurisdiction. The Company is prohibited from "tipping off" any vendor or user that a SAR has been or may be filed.

Important — Tipping Off Prohibition

The Company and all its personnel are strictly prohibited from informing any vendor, buyer, or third party that a Suspicious Activity Report has been, or is being considered for, filing with any authority. Disclosure of this nature may constitute a criminal offence under applicable law.

14.4 Cooperation with Authorities. The Company will cooperate fully with any competent regulatory authority, law enforcement agency, or court in connection with any investigation into suspected financial crime involving the Platform.

Section 15 — Data Retention

Record Type	Minimum Retention Period
KYC and identity verification records	Duration of vendor account plus seven (7) years after account closure
Transaction records and payout records	Seven (7) years from date of the relevant transaction
Sanctions and PEP screening records	Five (5) years from date of the screen

15.1 All KYC and identity verification records are retained for a minimum of the duration of the vendor's account plus seven (7) years after account closure, in accordance with the Privacy Policy v3.0 and applicable AML legislation.

15.2 Transaction records and payout records are retained for a minimum of seven (7) years from the date of the relevant transaction.

15.3 Sanctions and PEP screening records are retained for a minimum of five (5) years from the date of the screen.

15.4 Data is stored securely and access is restricted to authorised compliance personnel. All data handling is conducted in accordance with the Privacy Policy v3.0.

Section 16 — Escalation and Dispute Resolution

16.1 Right to Challenge KYC Decision. A vendor applicant whose application is declined on KYC/AML grounds, or a current vendor whose account is suspended or terminated for KYC/AML reasons, has the right to challenge that decision.

16.2 Escalation Process.

- 87. The vendor must submit a written challenge to the Company's compliance function within thirty (30) calendar days of the decision, setting out the grounds of challenge and any supporting documentation;
- 88. The compliance function will review the challenge within fifteen (15) business days of receipt of all required documentation;
- 89. Where the challenge cannot be resolved at compliance function level, it will be escalated to the Company's senior management for a final determination within a further fifteen (15) business days;
- 90. The Company's final determination following the escalation process is binding for the purposes of Platform access, without prejudice to the vendor's rights to seek a remedy through an appropriate regulatory authority or court.

16.3 Regulatory Complaints. Vendors may refer regulatory compliance concerns to the appropriate supervisory authority in their jurisdiction. The Company welcomes regulatory engagement and will cooperate fully with any regulatory enquiry.

Section 17 — Governing Compliance Framework

This Policy is designed to comply with the following laws, regulations, and guidelines:

Jurisdiction	Applicable Laws and Regulations
United States	Bank Secrecy Act (BSA); FinCEN regulations; USA PATRIOT Act; OFAC sanctions regulations; applicable Michigan state laws.
Nigeria	Nigerian Data Protection Act 2023 (NDPA); Money Laundering (Prevention and Prohibition) Act 2022; Terrorism (Prevention and Prohibition) Act 2022; Central Bank of

Jurisdiction	Applicable Laws and Regulations
	Nigeria (CBN) KYC and AML guidelines; Economic and Financial Crimes Commission (Establishment) Act 2004; Federal Competition and Consumer Protection Act (FCCPA).
United Kingdom	Proceeds of Crime Act 2002; Terrorism Act 2000; Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017; UK GDPR and Data Protection Act 2018; FCA guidance.
European Union	EU Anti-Money Laundering Directives (AMLD4 and AMLD5); GDPR; relevant national AML implementing legislation.
Canada	Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA); PIPEDA; FINTRAC regulations.
Other African Jurisdictions	The Company complies with applicable AML, KYC, and data protection legislation in all African jurisdictions from which vendors are onboarded.

Section 18 — General Provisions

18.1 Amendment. The Company reserves the right to amend this Policy at any time in response to changes in applicable law, regulatory guidance, or business requirements. Amendments will be communicated to vendors via the Vendor Dashboard and by email to registered addresses. Vendors are required to comply with the Policy as amended.

18.2 Severability. If any provision of this Policy is found to be invalid or unenforceable under applicable law, that provision shall be deemed severed from the Policy to the minimum extent necessary, and the remaining provisions shall continue in full force and effect.

18.3 Governing Law. This Policy shall be governed by and construed in accordance with the laws of the State of Michigan, United States of America, without prejudice to any mandatory regulatory requirements applicable in the vendor's or buyer's jurisdiction.

18.4 Contact. All compliance enquiries, KYC disputes, and data subject requests should be directed to:

Department	Compliance and Operations Team
Organisation	Afriq Global Market Limited
Email	davidsopekan@afriqglobal.org
Website	www.afriqglobal.org

18.5 Review Cycle. This Policy will be formally reviewed at least annually, or earlier upon any material change in applicable law, regulatory guidance, or the Company's payment, KYC, or logistics partner structure.

END OF VENDOR ONBOARDING AND KYC POLICY v2.0

EFFECTIVE: 1 SEPTEMBER 2026

AFRIQ GLOBAL MARKET LIMITED | www.afriqglobal.org

CONFIDENTIAL — INTERNAL COMPLIANCE DOCUMENT