



ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING (AML/CFT) POLICY

Version 1.0 Effective Date: 18 October 2026

1. Policy Statement

- 1.1 Kay's Limited, the operator of KaysPay, is committed to preventing the use of its services for money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction. This Policy summarises the measures we apply and the obligations of our customers.
- 1.2 We do not knowingly process any transaction connected with money laundering, terrorist financing, proliferation financing, fraud or any other unlawful activity.

2. Legal and Regulatory Framework

- 2.1 Our programme is based on the Money Laundering (Prevention and Prohibition) Act 2022, the Terrorism (Prevention and Prohibition) Act 2022, the AML/CFT regulations and guidelines of the Central Bank of Nigeria ("CBN") applicable to payment service providers, and the requirements of our licensed banking partner, 9 Payment Service Bank Limited ("9PSB").

3. Governance

- 3.1 Kay's Limited has designated a Compliance Officer, who also serves as Money Laundering Reporting Officer ("MLRO"). The Compliance Officer is responsible for the implementation of this Policy, for decisions on reports to the Nigerian Financial Intelligence Unit ("NFIU"), and for liaison with regulators.
- 3.2 The Compliance Officer may be contacted at support@kayspay.com.ng, with the message marked "Compliance".

4. Risk-Based Approach

- 4.1 We apply a risk-based approach. The extent of customer due diligence, monitoring and ongoing review is proportionate to the risk presented by the customer, the product, the delivery channel, the value and pattern of transactions and the geographic location involved.

5. Customer Due Diligence

- 5.1 We verify the identity of each customer before providing wallet services. The information required at each account tier is set out in our KYC Policy.
- 5.2 Enhanced due diligence applies to a customer who is a politically exposed person, who is connected with a jurisdiction identified as high risk, who requests unusually large funding or whose activity presents an unusual pattern. Enhanced due diligence may include requiring information on the source of funds and approval by the Compliance Officer before the relationship continues.



6. Sanctions and Politically Exposed Person Screening

- 6.1 We may screen customers and transactions, directly or through our banking and verification partners, against sanctions lists and lists of politically exposed persons. Where a sanctions match is confirmed, the account will be restricted and the matter escalated to the Compliance Officer.

7. Transaction Monitoring

- 7.1 We monitor wallet and transaction activity for unusual patterns by means of automated integrity checks and human review. Every wallet movement is recorded in a permanent ledger. An automated alert does not of itself result in the closure of an account and is reviewed by an authorised person.

8. Suspicious Activity Reporting

- 8.1 Where we know or suspect that activity may involve money laundering, terrorist financing or another criminal offence, we are required by law to report it to the NFIU or another competent authority.
- 8.2 We are prohibited from informing a customer that a report has been made or is under consideration. This prohibition on tipping off is a legal requirement.

9. Record Keeping

- 9.1 We retain customer identification records, transaction records and records of reports and screening decisions for at least seven years, or for longer where the law or a regulator so requires.

10. Staff Training

- 10.1 All personnel who handle customer funds, identity data or transaction records receive training on money laundering risks, warning indicators and escalation procedures on joining the company and at least annually thereafter.

11. Obligations of Customers

- 11.1 Customers must:
- (a) provide accurate information and keep it up to date;
 - (b) use their Account only for their own funds and for lawful purposes;
 - (c) not permit another person to use their Account or use KaysPay to move funds on behalf of another person;
 - (d) respond promptly to requests for information or documents, including information on the source of funds; and
 - (e) notify us of any activity on their Account that they do not recognise.



12. Restriction of Accounts

- 12.1 We may delay or refuse a transaction, or restrict an Account, where a sanctions match or credible politically exposed person match is confirmed, where suspicious activity is under review, where fraud is suspected or where a competent authority so requires.
- 12.2 A restriction prevents outgoing transactions and does not result in forfeiture of funds. Restrictions arising from suspected fraud or money laundering are decided or confirmed by the Compliance Officer. Where the law permits, the customer will be told how to respond.

13. Prohibited Use

- 13.1 KaysPay must not be used to move the proceeds of crime, to finance terrorism or proliferation, to evade sanctions or taxes, to pay for unlawful goods or services, or to conceal the true owner or source of funds. A breach may result in the closure of the Account and a report to the authorities.

14. Cooperation with Authorities

- 14.1 We cooperate with the CBN, the NFIU, the Economic and Financial Crimes Commission, the Nigeria Data Protection Commission and other competent authorities. Requests from authorities are handled by the Compliance Officer, who confirms the authority of the requester before any customer record is released.

15. Reporting a Concern

- 15.1 A person who suspects that KaysPay is being used for money laundering, fraud or any other offence may report it to support@kayspay.com.ng, marked "Compliance", or through the Contact Support option in the application, and may also report it to the NFIU or the Economic and Financial Crimes Commission.

16. Review

- 16.1 This Policy is reviewed at least annually, and whenever there is a material change in the law, in our services or in our risks.