

AML/CFT/CPF Policy Statement

Item	Detail
Issued by	Olympus Pay Proprietary Limited (registration BW00009700756)
Version	1.0, effective 12 October 2026
Approved by	Board of Directors
Next review	12 October 2027

Our commitment

Olympus Pay Proprietary Limited (Olympus) does not allow its accounts, payments, cards, merchant services, agent network or software to be used for money laundering, the financing of terrorism, the financing of the proliferation of weapons of mass destruction, or illicit dealing in arms or ammunition. We apply this commitment to every product, every channel and every person who works for us or acts on our behalf.

Legal framework

Olympus is a specified party under the Financial Intelligence Act, 2022 of Botswana, as amended in 2025. Our programme implements that Act and its regulations, including the Financial Intelligence (Implementation of United Nations Security Council Resolutions) Regulations, 2022, together with the Counter-Terrorism Act, the Proceeds and Instruments of Crime Act, the Banking Act and the Data Protection Act, 2024. We follow the guidance of the Financial Intelligence Agency (FIA) and the Bank of Botswana, which supervises Olympus as an admitted member of its Regulatory Sandbox, and the Recommendations of the Financial Action Task Force.

Our programme

Our Board of Directors approves our anti-money laundering, counter-terrorist financing and counter-proliferation financing (AML/CFT/CPF) policies and oversees how they work. A Compliance Officer at management level runs the programme, reports to the Board, and is our contact point for the FIA and the Bank of Botswana. The programme is built on six written policies that cover:

- governance, risk appetite and the businesses we will not serve;

- customer due diligence, including electronic identity verification, beneficial ownership and enhanced checks for higher-risk customers;
- targeted financial sanctions and counter-proliferation financing;
- the reporting of suspicious and threshold transactions;
- assessment of the risks we face, including before we launch a new product;
- record keeping, staff training and independent review.

Knowing our customers

We identify and verify every customer before we open an account or carry out a transaction. Individuals are verified electronically with a government identity document, a live selfie and biometric matching. For companies, partnerships, societies and trusts, we verify that the entity exists, who controls it, who may act for it, and every natural person who ultimately owns or controls it. We ask about the purpose of the account and where the money comes from, and we keep this information up to date for as long as the relationship lasts.

We apply enhanced due diligence to higher-risk customers, including Prominent Influential Persons, their family members and close associates, and customers connected with high-risk countries or businesses. These relationships need senior management approval and are monitored more closely.

Sanctions

We screen every customer, beneficial owner, director and signatory, and relevant payments, against United Nations Security Council sanctions lists and the persons listed by the Minister under Botswana law, at onboarding and on an ongoing basis. We also screen against other major international sanctions lists. Where we find a designated person, we freeze their funds without delay and report to the FIA.

Monitoring and reporting

We monitor transactions for activity that does not match what we know about a customer. We report suspicious transactions and activity to the FIA through its goAML reporting system, as well as the cash and cross-border transactions the law requires us to report. By law, we cannot tell anyone that a report has been made or may be made.

Records, training and review

We keep identification and transaction records for the period the Financial Intelligence Act requires, which is 20 years. Every employee is trained when they join and every year, and our programme is tested independently. We review these policies at least once a year and whenever the law, our products or our risks change.

What this means for you

- We may ask you for information or documents when you open an account and from time to time afterwards. Please keep your details up to date.
- We may delay, decline or stop a transaction, or restrict or close an account, where the law or our policies require it. In some cases we cannot tell you why.
- We will never ask you for your password or one-time codes as part of these checks.

Contact

Questions about this statement can be sent to legal@olympuspay.co, marked for the attention of the Compliance Officer, or to Olympus Pay Proprietary Limited, Plot 69184, Block 8, Science and Technology Park, Gaborone, Botswana.