Anti-Money Laundering Policy

Introduction

As a company, we understand the importance of preventing money laundering and terrorist financing and adhere to carrying on business in accordance with the highest standards of anti-money laundering and terrorist financing in Nigeria.

Jupit Technologies, as a FinTech company, is subject to the regulatory framework designed to prevent money laundering in Nigeria. This framework includes such laws as: Terrorism Prevention Act 2103, Money Laundering Prohibition Act 2011 (as amended) and others. To meet this commitment, Jupit Technologies has put in place some policies and procedures. This document sets forth the company's expectations for its users, employees, and other business partners.

Our Policy Statement on AML and CTF

It is Jupit's policy to comply with all Anti-Money Laundering and Combating Terrorist Financing Laws applicable to our operations in Nigeria. To this end, Jupit Technologies will only conduct business with users and partners who are involved in legitimate business activity and whose funds are derived from legitimate sources.

This Policy is intended to prevent money laundering, including the need to have adequate systems and controls in place to mitigate the risk of the firm being used to facilitate financial crime and to help our users and employees to understand where breaches of AML Laws might arise and to support them in making the right decisions in line with our corporate position as stated in this Policy.

Who is subject to this Policy?

This Policy applies to all Jupit's operations, including all legal entities owned or controlled by Jupit, and to all directors, employees, users, and other third parties acting on behalf of the foregoing.

What do we mean by Money Laundering and Terrorist Financing?

Money laundering is the processing of criminal proceeds to disguise their illegal origin. This process involves cleaning money generated by criminal activity, such as drug trafficking, terrorist funding or cyber-fraud, to appear to have come from a legitimate source.

Terrorism Financing is defined as providing, depositing, distributing or collection funds, directly or indirectly, intended to be used, or knowing that these funds are to be wholly or partially use, for the committing of terrorist acts.

The following types of activities are considered to be “money laundering” and are prohibited under this Policy:

a) the transfer of funds to a Jupit account knowing or suspecting that such funds is derived from criminal or certain specified unlawful activity, for the purpose of disguising the illicit origin of the funds;

b) conducting any type of exchange transaction which involves criminally acquired funds;

c) the concealment or disguise of the true nature, source, disposition, transfer, rights with respect to ownership or control of criminal funds;

d) promoting the carrying on of unlawful activity; and

e) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points.

Red Flags

Where any suspicions arise that criminal conduct may have taken place involving a user, employee or third party, you should consider whether there is a risk that money laundering or terrorist financing has occurred or may occur.

Some examples of red flags to be reported include:

- A user provides insufficient, false or suspicious information or is reluctant to provide complete information

- Methods or volumes of payment that are not consistent with the payment policy or that are not customarily used in the course of business, e.g., cash deposit by third party, payments with cheques, and/or payment transfer from unrelated third parties

- Structuring transactions to avoid government reporting or record keeping requirements

- Wire transfer activity that is not consistent with the activities of the customer, or which originates or terminates with parties unrelated to the transaction

- Unexpected spikes in a customer's activities

What's the Risk?

Violating the Anti-money laundry laws may lead to severe civil and criminal penalties. These could include hefty fines, imprisonment, extradition, blacklisting, and the revocation business operation. In addition, violations of AML laws can have substantial consequences, such as damage to reputation and commercial relationships, restrictions in the way we can business, and the enormous time and cost of conducting internal investigations and/or defenses against government investigations and enforcement actions.

Compliance Controls

Jupit is responsible for ensuring that its business has a culture of compliance and effective controls to comply with AML laws and regulations to prevent, detect and respond to money laundering and counter-terrorism financing and to communicate the serious consequences of non-compliance to employees and users.

Know Your Customer (KYC) Procedures

Jupit Technologies is strongly committed to complying with all the applicable anti-money laundering rules within the regulatory framework and in order to adhere to these regulatory standards and to aid in prevention of money laundry or terrorist financing, Jupit will implement processes and procedures in its Line of Businesses (LOBs) to conduct appropriate customer due diligence ("DD") on the basis of the following “Know Your Customer” principles: ·

- Customer Personal Details (Account Opening);
- Bank Verification Number (Verification Checking);
- Valid Government Issued Identity Card and Selfie (Ownership Verification).

As an extra measure to the procedure, Jupit may perform enhanced due diligence procedures for customers presenting a higher risk, such as those transacting large volumes frequently etc. Unusual activity during the customer due diligence process or customer engagement should be reported immediately to the designated Jupit Compliance department or Commercial department.

Applicable Regulatory Framework

Jupit complies with all applicable AML/CTF laws and regulations, Financial Action Task Force (FATF) Recommendations and additional local AML regulations as required.

Non-compliance

Any Jupit employee or customer, who violates this Policy may be subject to appropriate disciplinary action, independently from potential other penalties resulting from their behavior.

Internal Audit shall conduct regular checks on business operations to ensure compliance with AML Laws.

Updates, Review and Ownership

This Policy may be updated from time, and the updated version of the Policy will be immediately made available on the Jupit website.