



SAURIPAY

Anti-Money Laundering Policy

April, 2025

Content of this AML Policy

1.	Anti-Money Laundering (AML)/ Combating Financing of Terrorism (CFT) Policy Statement.....	3
2.	Objectives	3
3.	Legal Framework.....	4
4.	Risk-based approach	4
5.	Customer due diligence (CDD/KYC)	5
6.	Enhanced due diligence (EDD)	5
6.1.	High-risk situations.....	6
6.2.	Politically Exposed Persons (PEPs).....	6
7.	On-going monitoring	7
8.	AML Training and Awareness.....	8

1. Anti-Money Laundering (AML)/ Combating Financing of Terrorism (CFT) Policy Statement

SauriPay, operating in Nigeria and regulated by the Nigerian Laws makes every effort to remain in full compliance with all applicable Anti-Money Laundering laws, rules and standards in force in Nigeria.

For the purposes of this Policy, Money Laundering is defined as a process in which the proceeds of crime are transformed into ostensibly legitimate money or assets. It involves the introduction of assets derived from illegal and criminal activities (predicate offences) into the legal financial system and business cycle. These predicate offences include drug trade, child trafficking, forgery of money, organized crime etc. Financing of Terrorism is defined as provision of funds directly or indirectly knowing that the funds are to be used to fund terrorist acts or organizations.

This Policy applies to all **SauriPay** employees, all units in the **SauriPay**, senior management, foreign correspondents, contractors and third parties with whom **SauriPay** may contract with.

To facilitate compliance with Anti-Money Laundering requirements, **SauriPay** has:

- i. Developed and implements written Anti-Money Laundering Policy, procedures, internal controls and systems, which include but are not limited to:
 - customer identification program and procedures;
 - procedures to collect and refresh, as appropriate, customer due diligence information;
 - processes to assess risk at both the program and customer level;
 - processes and systems to monitor customer transactions and activity;
 - processes and systems to identify and report suspicious activity; and
 - processes to keep required records.
- ii. Developed a program to train employees in Anti-Money Laundering detection and prevention procedures.
- iii. **SauriPay** cooperates fully with law enforcement and regulatory investigations and inquiries, does not do business with blacklisted entities/ jurisdictions and is compliant with all legal provisions.
- iv. **SauriPay** fully complies with applicable Anti-Money Laundering Laws, Regulations and Circulars etc.

2. Objectives

SauriPay is committed to the highest standards of Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) compliance and requires Management and employees to adhere to these standards to prevent use of its products and services for money laundering/ terrorist financing purposes.

SauriPay will examine its AML/CFT strategies and objectives on an ongoing basis and maintain an effective AML/CFT policy that reflects best practices. Compliance with this policy is the responsibility of all Directors, Management and employees.

SauriPay's AML program includes clients screening and monitoring requirements, Know Your Customer (KYC) policies, sanctions policy, record-keeping requirements, reporting of suspicious transactions in accordance with established AML/CFT framework.

The standards set out in this policy are minimum standards based on applicable legal and regulatory requirements and applies to **SauriPay**. The requirements are intended to prevent **SauriPay**, its employees and clients from being used for money laundering, terrorist financing or other financial crime. Thus, the Policy establishes the general framework for the fight against money laundering and financing of terrorism.

3. Legal Framework

The legal framework for AML/CFT program consists of (including but not limited to):

- Money Laundering (Prevention and Prohibition) Act, 2022
- Terrorism Preventing and Prohibition Act, 2022
- Nigerian Financial Intelligence Unit (NFIU) Act, 2018
- Economic and Financial Crimes Commission (EFCC) Act, 2004
- Central Bank of Nigeria (CBN) AML/CFT Regulations (such as the Central Bank of Nigeria (CBN) AML/CFT/CPF Regulations, 2022; the CBN Customer Due Diligence Regulations, 2023; the CBN Guidance Notes on Politically Exposed Persons, etc.)
- Securities and Exchange Commission (SEC) AML/CFT Guidelines
- Special Control Unit Against Money Laundering (SCUML) Guidelines
- The Financial Action Task Force (FATF) Recommendations, United Nations Security Council resolutions and other international instruments.

4. Risk-based approach

Risk may be established both on the basis of objective criteria and subjective criteria. A 'risk rating' is given to each criterion.

SauriPay, as part of its AML program, has conducted a risk analysis to identify specific criteria of potential money laundering risks. This risk-based approach includes the identification of the money laundering and terrorist financing risks (to the extent that such terrorist financing risk can be identified) of customers, categories of customers, and transactions that allow **SauriPay** to determine and implement proportionate measures and controls to mitigate these risks. While a risk assessment is routinely performed at the inception of a customer relationship, for some customers a comprehensive risk profile may only become evident once the customer has begun transacting through an account. Thus, the monitoring of customer transactions and ongoing reviews is a fundamental component of **SauriPay's** risk-based approach. In addition, this type of risk assessment process may also be adjusted for a particular customer based upon information received from a competent authority.

SauriPay measures money laundering and terrorist financing risks using the Low Risk, Medium Risk and High Risk categories. The application of risk categories provides a strategy for managing potential risks by enabling **SauriPay** any to subject customers to proportionate controls and oversight. The weight given to these risk categories (individually or in combination) in assessing the overall risk of potential money laundering may vary depending on **SauriPay**'s unique circumstances.

To all customers classified as High Risk the procedure of enhanced due diligence is applied. The main criteria to rank the client as high risk are the following:

- the high risk jurisdiction domiciles of customers;
- the high risk or prohibited industries or activities of customers; complex shareholder structure with hidden UBOs;
- PEPs as shareholders or key management personnel;
- restrictions or sanctions imposed on customers by relevant regulatory authorities;
- nonresident customers;
- Politically Exposed Persons (PEPs) accounts;
- customers from countries that are considered by the FATF inadequately to apply the FATF Recommendations;
- transactions that are unusual, lack an obvious economic or lawful purpose;
- transactions that are complex or large or might lend themselves to anonymity; trusts, charities, NGOs and organization receiving donations;
- any other customers that their nature entail a higher risk of money laundering or terrorist financing;
- customers with dubious reputation as per public information available.

5. Customer due diligence (CDD/KYC)

Customer due diligence (CDD) is central to an effective anti-money laundering and counter- terrorism financing (AML/CTF) regime. **SauriPay** takes measures to identify and verify each of its customers so it can:

- determine the money laundering and terrorism financing risk posed by each customer;
- decide whether to proceed with a business relationship or transaction;
- assess the level of future monitoring required.

SauriPay has implemented a KYC program to ensure all kinds of customers (natural or legal persons or legal structures) are subject to adequate identification, risk rating and monitoring measures. This program has been implemented throughout all **SauriPay** divisions. The purpose of this is to reduce the risk of the **SauriPay** being used for money laundering and financing of terrorism.

6. Enhanced due diligence (EDD)

SauriPay applies an Enhance Due Diligence where the customer and product/service combination is considered to be a greater risk. This higher level of due diligence is required to mitigate the increased risk. A high risk situation generally occurs where there is an increased opportunity from money laundering or terrorist financing through the service and product **SauriPay** provides or from a customer of **SauriPay**.

What the enhanced due diligence actually entails will be dependent on the nature and severity of the risk.

6.1.High-risk situations

In any situation that by its nature presents a higher risk of ML/TF, **SauriPay** takes additional measures to mitigate the risk of ML/TF.

Additional measures or EDD may include:

- obtaining additional information on the customer (e.g. connected parties, accounts or relationships) and updating more regularly the customer profile including the identification data;
- obtaining additional information on the intended nature of the business relationship (e.g. anticipated account activity), the source of wealth and source of funds;
- obtaining the approval of senior management to commence or continue the relationship; and
- conducting enhanced monitoring of the business relationship, by increasing the number and timing of the controls applied and selecting patterns of transactions that need further examination.

6.2.Politically Exposed Persons (PEPs)

In order to reduce possible risks **SauriPay** conducts EDD at the outset of the business relationship and ongoing monitoring where it knows or suspects that it has business relationship with a PEP.

The definition of 'PEP' is set out below:

- Is or has, at any time in the preceding year, been entrusted with prominent public functions;
- Is an immediate family member of such a person Is a known associate of such a person;
- Is or has, at any time in the preceding year, been entrusted with a prominent public function by:
 - Any state;
 - The European Community; or
 - An international body; or
 - An immediate family member or a known close associate in cases where PEP is identified.

Senior management approval should always be sought before establishing a business relationship with a PEP and the source of funds should be established. The business relationship should be subject to enhanced and constant monitoring.

It is important that before a business relationship is entered into with a PEP their source of funds is established and **SauriPay** is satisfied that there are no indications that funds that will be used for transactions to be carried out are derived from corruption (i.e. receipt of bribes), fraud or an attempt by the PEP to remove/hide assets from their homecountry. The source of the PEP's funds may be established by asking the individual concerned a series of questions to determine from where they receive their money. These questions could include confirmation of the main source income (i.e. salary), any business interest or investments from which funds are/will be received.

Establishing the customer's source of wealth or source of funds is a core requirement of EDD. Source of wealth refers to the origin of an individual's entire body of wealth (i.e. total assets). This information will usually give an indication as to the size of wealth the customer would be expected to have, and a picture of how the individual acquired such wealth. Although **SauriPay** may not have specific information about assets not deposited with or processed by it, it may be possible to gather general information from the individual, commercial databases or other open sources.

7. On-going monitoring

Effective ongoing monitoring is vital for understanding of customers' activities and an integral part of effective AML/CTF systems. The extent of monitoring is linked to the risk profile of the customer which has been determined through the risk assessment procedures and is dedicated to regularly reassess clients and their transactions to make sure their suspicion level remains justified. **SauriPay** applies an Enhance Due Diligence where the customer and product/service combination is considered to be a greater risk. This higher level of due diligence is required to mitigate the increased risk.

SauriPay takes additional measures when monitoring business relationships that pose a higher risk. High-risk relationships, for example those involving PEPs, will require more frequent and intensive monitoring.

Monitoring of customers: **SauriPay** continuously monitors its business relationship with a customer by:

- reviewing client's profile at frequency defined by the client's risk category to ensure that they are up-to-date and relevant;
- monitoring the activities of the customer to ensure that they are consistent with the nature of business, the risk profile and source of funds.

An unusual transaction may be in the form of activity that is inconsistent with the expected pattern for that customer, or with the normal business activities for the type of product or service that is being delivered.

Transaction monitoring: **SauriPay** conducts an on-going transaction monitoring on a risk-based approach and considers:

- the nature and type of transactions (e.g. abnormal size or frequency);
- the nature of a series of transactions;
- the amount of any transactions;
- the geographical origin/destination of a payment;
- the customer's normal activity or turnover.

SauriPay is vigilant for changes on the basis of the business relationship with the customer over time, which may include:

- new products or services that pose higher risk are entered into;
- new corporate or trust structures are created;
- the stated activity or turnover of a customer changes or increases;
- the nature of transactions changes or their volume or size increases etc.

When considering how best to monitor customer transactions and activities, **SauriPay** takes into account the followings: the size and complexity of its business; its assessment of the ML/TF risks arising from its business; the nature of its systems and controls; the monitoring procedures that already exist to satisfy other business needs; the nature of the products and services (which includes the means of delivery or communication).

8. AML Training and Awareness

SauriPay maintains an on-going employee training program so that the staff is adequately trained in KYC procedures and that the staff is aware of different possible patterns and techniques of money laundering which may occur in their everyday business. Training requirements should have a different focus for new staff, front-line staff, compliance staff or staff dealing with new counterparties. New staff is educated in the importance of KYC policies and the basic requirements at **SauriPay**.

Training is given to all staff members upon commencement of taking on the position in the **SauriPay** and on regular occasions afterwards (at least once a year). Staff members who deal directly with the customers are trained to verify the identity of new customers, to exercise due diligence in handling accounts of existing customers on an on-going basis and to detect patterns of suspicious activity. Training also covers the general duties arising from applicable external (legal and regulatory), internal requirements and the resulting individual duties which must be adhered to in everyday business as well as typologies to recognize money laundering or financial crime activities or sanctions violation typologies.

SauriPay conducts annual AML training for all employees. This training is designed to ensure that employees:

- Understand applicable AML legislation, including relevant laws;
- Are familiar with the company's AML policies, procedures, systems, and controls, including any recent updates;

- Can identify and appropriately handle transactions or activities that may indicate money laundering;
- Stay informed about current methods, techniques, and trends in money laundering relevant to the company's operations;
- Are aware of key findings, recommendations, guidelines, directives, sanctions, notices, and other relevant developments in the AML field.

SauriPay ensures that its AML training is appropriately tailored to the company's activities, including its products, services, customers, distribution channels, business partners, and the level and complexity of its transactions. The training also highlights the different levels of money laundering risk and vulnerabilities associated with the aforementioned areas.

9. Record keeping

SauriPay takes reasonable measures to prevent loss or destruction of records, prevent their falsification, detect and correct any inaccuracies contained in them and prevent unauthorized persons from accessing or using the information contained in them. All records of business transactions are held for at least five years from the date that the business relationship ends.

The records to be kept include a copy of or references to the evidence of the customer's identity obtained under customer due diligence requirements, supporting records of business relationships or occasional transactions subject to due diligence or ongoing monitoring, the date and method of the initial client identification and verification, and any documents justifying exemption from identification, if applicable.

In relation to the evidence of a customer's identity, businesses must keep the following records:

- a copy of the identification documents accepted and verification evidence obtained, or
- references to the evidence of customer's identity.

Transaction and business relationship records (for example, account files, relevant business correspondence and so on) should be maintained in a form from which a satisfactory audit trail may be compiled, and which may establish a financial profile of any suspect customer.