PremiumTrust Bank

...Together for Growth

www.premiumtrustbank.com

ANTI-MONEY LAUNDERING/COMBATING THE FINANCING OF TERRORISM/COUNTERING PROLIFERATION FINANCING POLICY

PremiumTrust Bank

APPROVAL

Action	Name	Title	Signature	Date
Prepared By	Cosmas Uwaezuoke	Chief Compliance Officer		16/6/23
Recommended By	Emmanuel Emefienim	MD/CEO		16/06/23
Recommended By	Neville Afigan	Chairman, Board Risk Management Committee		16/06/23
Approved By	Perez Araka	Chairman, Board of Directors		16/06/23

TABLE OF CONTENT

- Money Laundering (Prevention and Prohibition) Act 2022
- Terrorism (Prevention and Prohibition) Act 2022
- Proceeds of Crime (Recovery and Management) Act 2022
- CBN AML/CFT/CPF Regulation 2022
- Company and Allied Matter Act 2020
- Banking and Other Financial Institutions Act (BOFIA) 2020
- Various Other Regulations

3	**Definitions of Terms** ML: Money Laundering TF: Terrorist Financing PF: Proliferation Financing AML: Anti-Money Laundering CFT: Combating the Financing of Terrorism CPF: Countering Proliferation Financing CBN: Central Bank of Nigeria FATF: Financial Action Task Force NFIU: Nigerian Financial Intelligence Unit KYE – Know Your Employee KYC – Know Your Customer EDD – Enhanced Due Diligence CDD – Customer Due Diligence	

Section 1: Overview of the AML/CFT/CPF Policies

1.1 Introduction

The Anti-Money Laundering, Combating Terrorism Financing, and Countering Proliferation Financing (AML/CFT/CPF/CPF) policy ("The Policy") covers all staff of PremiumTrust Bank Limited ("The Bank").

The policies herein embody good business practice and reflect the high-level principles for businesses laid down by the Central Bank of Nigeria. It is essential for Premium Trust Bank Limited to maintain a high reputation for professionalism and for acting in accordance with extant regulations and global best practices.

This Policy document contains the basic standards of Anti-Money Laundering, Combating Financing of Terrorism and Countering Proliferation Financing of Weapons of Mass Destruction (hereinafter collectively referred to as AML/CFT/CPF) within Premium Trust Bank Limited.

All the Bank's employees shall be familiar with and make use of the materials contained in this Policy while copies shall be made available to all the Departments of the Bank.

Compliance with the provisions of this policy will help to build a culture of compliance in Premium Trust Bank Limited.

1.2 Scope

This Policy is the PremiumTrust Bank Limited AML/CFT/CPF Policy and is applicable to the Bank. It provides principles and minimum standards from a risk-based approach to proactively identify money laundering, terrorist financing and proliferation financing risks that face the Bank and to ensure that controls, mechanisms and monitoring processes are in place to help in mitigating these risks thus contributing to the global combat against money laundering, terrorist financing and proliferation financing.

It should be noted that these standards are minimum and as such whenever the applicable local money laundering, terrorist financing and proliferation laws establish a higher standard; the Premium Trust Bank Limited shall adhere to those higher standards.

1.3 Purpose

The essence of this policy is to:

I. Document the comprehensive and constantly evolving, policies, procedures and processes deployed by Premium Trust Bank Limited to assure adherence to the provisions of AML/CFT legislations and guidelines in all our business locations:
II. Create a framework for managing compliance risks in the bank.
III. Ensure that the bank does not fall victim of illegal activities perpetrated by its customers:
IV. Specify basic expectations of all staff regarding their obligations for the management of ML/TF/PF risk, Know Your Customer (KYC) identification and customer onboarding procedure, detecting, and reporting suspicious as well as unusual transactions and activities.
V. Prescribe measures to comply with applicable statutory and regulatory requirements and prevent regulatory sanctions against the Bank.
VI. Provide a guide aimed at preventing money laundering, terrorist financing, proliferation financing activities within the Bank.
VII. Provide our products and services only to customers whose identities and the nature of the business transactions have been reasonably ascertained.

VIII. Avoid relationships with those that we reasonably assess as posing unacceptable risks of money laundering, terrorism financing or proliferation financing.

IX. Assess the viability of maintaining ongoing relationships with customers that fit these criteria.

X. Assign clear AML/CFT/CPF responsibilities, relevant to staff respective roles and areas, as appropriate.

XI. Monitor, measure, and report compliance with our AML/CFT/CPF Program and take corrective actions as necessary.

It should be noted that this Policy is not a static document; it will continue to change to reflect changes in both the laws and regulation itself and in best practice, and staff should expect to receive regular updates.

1.4 Policy Statement

Premium Trust Bank is committed to:

I. The highest standards of Anti-Money Laundering, Countering the Financing, of Terrorism and Countering Proliferation Financing (AML/CFT/CPF) policies and procedures including Anti-Human Trafficking, Anti-Bribery and Corruption, Anti-Fraud, Anti-Slavery, and other punishable criminal acts which will ensure that it is not used as a conduit for money laundering or terrorist financing and proliferation financing of other illicit businesses:

II. Implementing policies, procedures, guidelines and provisions of applicable laws, regulations, circulars and guidance notes emanating from the Government and relevant regulatory bodies towards ensuring compliance with all domestic and international laws regulations on money laundering, terrorist financing and proliferation financing to mitigate the inherent risk it is exposed to:

III. Full compliance with both the letter and the spirit of all regulatory requirements and high standard of market conduct.

IV. Conducting all banking and investment business in accordance with all regulatory policies and guidelines governing its operating environment.

V. Giving full cooperation to Law Enforcement Authorities within the limits of the rules governing confidentiality.

VI. Effective communication of these policies towards raising the level of staff awareness on AML/CFT/CPF issues.

VII. Retention and preservation of records of customers' transactions for a minimum period of five years or as may be prescribed by various regulatory bodies.

VIII. Exiting relationships which pose heightened money laundering risks to the bank and reporting same to the relevant regulatory agencies.

Drawing significantly from recommendations of the Money Laundering (Prevention and Prohibition) Act 2022 (MLPPA), Terrorism (Prevention and Prohibition) Act 2022 (TPPA), Central Bank of Nigeria (Anti-money Laundering, Combating the Financing of Terrorism and Countering Proliferation Financing of Weapons of Mass Destruction in Financial Institutions in Nigeria) AML/CFT/CPF Regulations, 2022,, Financial Action Task Force 40 Recommendations, the Wolfsberg Group principles, recommendation of the Basel Committee on Banking Supervision, Local, Cultural and environmental factors and other international best practices, the Bank has

put in place the following measures in the attainment of its objective of ensuring full compliance with the letter and the spirit of all applicable laws and regulations.

The Bank

I. Has established sound internal policies, controls, procedures to prevent/ mitigate money laundering, financing of terrorism as well as bribery and corruption, fraud, and human trafficking risks.

II. Confirms that it supports anti-slavery courses, does not make use of slaves as staff, and does not permit its services for slavery or human trafficking transactions or purposes.

III. Regularly trains its staff to identify unusual and suspicious activities/transactions and to take appropriate actions.

IV. Has in place an AML/CFT/CPF employee training programs for new hires and regular refresher training for existing staff.

V. Has an internal referral process and procedure for compliance matters.

VI. Ensures implementation of policies and procedures and internal controls to correct/enhance and/or adapt to regulatory changes / deficiencies.

VII. Has designated a senior management staff as its Chief Compliance Officer to oversee its AML/CFT/CPF program.

The Bank understands that the fight against money laundering, terrorism/terrorist financing and proliferation financing is the collective responsibility of all stakeholders and as such takes its role very seriously.

This policy refers to the Bank's approach to ensuring that it can effectively identify, verify, and monitor its customers and the financial transactions in which they engage, relative to the risks of money laundering, terrorism financing and proliferation financing.

1.5 Roles and Responsibilities

1.5.1. The Bank

The Bank is responsible for (but shall not be limited to):

- The Bank shall document applicable policies and processes on Anti-Money Laundering /Combating Terrorism Financing/ Counter Proliferation Financing. These policies shall be hosted on the Bank's intranet to ensure that they are readily available to all staff.
- The Bank shall ensure that it puts an effective compliance program in place.
- The Bank shall ensure that staff are properly trained to enable them to carry out their relevant roles as it relates to Anti-Money Laundering /Combating Terrorism Financing/ Counter Proliferation Financing.
- Ensure proper record-keeping processes and systems.
- Ensure prompt cooperation with regulators and Law Enforcement Agencies.

1.5.2. The Board of Directors

They are responsible for (but shall not be limited to):

- Assume overall accountability for compliance performance.

- Ensure the appropriate AML/CFT/CPF Compliance Risk Management Framework is established and is in operation.
- Approve the AML/CFT/CPF Compliance Risk Management programs and policies.
- Supervise the implementation of the AML/CFT/CPF program, risk management and reporting requirement.
- Approving/setting policies, procedures, and setting the tone for Anti-Money Laundering /Combating Terrorism Financing/Countering Proliferation Financing and compliance culture within the entire Bank
- Appoint and designate a Chief Compliance Officer (in line with CBN guidelines) and coordinate and monitor the AML/CFT/CPF compliance by the Bank.
- Ensuring that the Chief Compliance Officer has a clear and accurate job description, and sufficient resources to perform his/her responsibilities.
- Seeking Annual Money Laundering Compliance Reports from the Chief Compliance Officer and acting on the findings within those reports.
- Assessing annually, the adequacy of the AML compliance function of the bank.

1.5.3. Members of Executive and General Management.

They are responsible for (but shall not be limited to):

- The day-to-day compliance with Money Laundering obligations within the areas of the Bank for which they are responsible. This includes ensuring that relevant staff are adequately trained in Money Laundering prevention, Know Your Customer (KYC) and reporting requirements.
- Ensuring that the Chief Compliance Officer has adequate resources to carry out his/her responsibilities including support staff and materials.
- Setting the tone by demonstrating explicit support for the Bank's Anti-Money Laundering/Combating Financing of Terrorism policies, Countering Proliferation Financing by enforcing strict adherence throughout the Bank.

1.5.4. Executive Compliance Officer (ECO)

He/She is responsible for (but shall not be limited to):

- This role must be occupied by an Executive Director
- The ECO shall report directly to the Board on all compliance related matters.
- Oversees the management of the Bank's Compliance risk.
- Review the Bank's AML/CFT/CPF and compliance policies.
- Facilitates compliance with the regulatory requirements on AML/CFT/CPF board's training and lends necessary support to Board members on area requiring further clarification.
- Provide adequate support for the CCO and staff members of the department.
- Ensure an adequate supervisory role over the Chief Compliance Officer and his/her activities.
- Promotes Compliance Culture in the Bank.
- Responsible and Accountable for any breach of extant regulation in the Bank.

1.5.5. Chief Compliance Officer (CCO)

He/She is responsible for (but shall not be limited to):

- Coordinate and monitor AML/CFT/CPF Compliance of the Bank.
- Inform the Board and Management of AML/CFT/CPF compliance efforts, compliance failures and status of corrective actions.
- Ensure implementation of Board's decision on compliance matters.
- Developing and maintaining Anti-Money Laundering/Combating Financing of Terrorism and Countering Proliferation Financing Policies and Procedures of the Bank in line with statutory and regulatory obligations.

- Undertaking, in consultation with senior management, an assessment of the vulnerability of the Bank to money laundering and terrorist financing risks and ensuring that this assessment remains up to date.
- Advising the Bank's management on all matters relating to Money Laundering / Terrorist Financing/ Proliferation Financing (ML/TF/PF)
- Preparing Quarterly Compliance Reports for each quarter and presenting it to the Board within a reasonable time thereafter.
- Monitoring changes in laws and regulations, examining trends and keeping staff informed of all relevant matters.
- Vigilance in computerized and non-computerized transactions and track patterns
- Maintaining up-to-date list of high-risk countries and identifying for the Bank, the high, moderate, and low risk activities from AML/CFT/CPF angle
- Ensuring that Whistle Blowing framework is functional and all Stakeholders are aware of its existence.
- Overseeing the Bank's compliance education programs by creating Anti-Money Laundering/Combating Terrorism Financing / Proliferation Financing awareness amongst staff aimed at ensuring that all members of staff know the rules and regulations on Money Laundering/ Terrorist Financing/ Proliferation Financing (ML/TF/PF) and are aware of their obligations and the Bank's procedures.
- Arranging and participating in necessary Anti-Money Laundering/Combating Terrorism Financing/Countering Proliferation Financing prevention training and awareness for staff at all levels.
- Being involved in the prior assessment of the regulatory compliance of all products of the Bank to ensure compliance with Anti-Money Laundering/Combating Terrorism Financing/Countering Proliferation Financing laws and regulations.
- Monitor the day-to-day operationalization of the Bank's AML policies and procedures.
- Rendering statutory reports to the NFIU, CBN and other regulators.
- Undertaking the internal review of all suspicious reports and determining whether such reports have substance and require disclosure to the NFIU and other regulators.
- Representing the Bank to all external agencies in Nigeria (CBN, NDIC, NFIU, NDLEA), and in any other third-party enquiries in relation to money laundering prevention, terrorist financing and proliferation financing investigation or compliance.
- Responding promptly to requests for information made by regulatory and law enforcement agencies.
- Ensuring all employees complete an annual AML compliance training.

1.5.6. Compliance Team Function

Members of the Compliance team are directly responsible for (but shall not be limited to):

- Ensuring the day-to-day implementation of Anti-Money Laundering obligations in the Bank.
- Taking responsibility for ensuring that the branch/department complies fully with all Anti-Money Laundering/Combating Terrorism Financing/Countering Proliferation Financing regulations as well as policies and procedures of the Bank.
- Providing the Chief Compliance Officer with all returns under the Money Laundering (Prevention and Prohibition) Act, 2022 (as amended) and all other subsisting regulations.
- Reporting directly to the Chief Compliance Officer on matters relating to money laundering, terrorist financing and proliferation of weapons of mass destruction.
- Responding promptly to requests for information made by the Chief Compliance Officer or regulatory authorities.
- Ensuring that all Know Your Customer/Know Your Customer's Business information is in place.
- Development of robust compliance framework, policies, and risk management strategy

- Identification, assessment, monitoring, management and mitigation of financial crime and compliance risks within the Bank
- Ensure institutionalization of AML/CFT/CPF and Regulatory Compliance via independent review, evaluation, and resolution.
- Monitoring of emerging and external events to determine exposures and risk indicators using a risk-based approach and creating awareness among all staff.
- Collaborate with other departments on the implementation of Corporate Governance, Conduct & Ethics principles, and anti-money laundering strategies across all strata of the bank.
- Create awareness among all staff and relevant stakeholders of the Bank's compliance risk exposures and ways of preventing these from crystallizing.
- Establish a compliance culture through staff training and awareness programs.
- Advisory services to board, senior management, and staff on compliance & corporate governance issues
- Periodic management information system reports on the bank's level of compliance.
- Regulatory liaison, customer information management and reporting in line with regulation
- Identification of potential areas of compliance vulnerability and risk; develop/implement corrective action plans for resolution of issues and provide general guidance on compliance activities.
- Compliance monitoring to ensure the Bank is not being used for the laundering of funds, financing of terrorist activities or proliferation.
- Management and monitoring of the Rule Book / Regulatory Universe
- Monitoring and driving compliance with Ethics & Sustainability requirements.
- Monitoring and driving compliance with Anti-Bribery & Corruption requirements.
- Keeping pace with evolving industry practices and local/international regulation
- Ensuring that the Bank's policies and procedures reflect current regulatory and best practice requirements.
- Compliance review of branches and departments.
- Contact point for regulatory authorities and law enforcement agencies regarding AML/CFT/CPF and other Compliance related issues.
- Gatekeeper in preventing money laundering, financing of terrorism and proliferation financing.
- Product review and AML risk assessment
- Conduct Financial Institutions due diligence reviews and certification.
- Management of the Bank's sanction program
- Preparation of management and board reports
- Monitoring, reviewing, and reporting Suspicious Transactions
- Reviewing of staff accounts
- Any other responsibilities that may be assigned by the Chief Compliance Officer

1.5.7. All Employees

Each staff is responsible for (but shall not be limited to):

- Be familiar with and comply with applicable laws and regulations.
- Being conversant with the Anti-Money Laundering/Combating Terrorism Financing and Countering Proliferation Financing laws, and regulations. Staff should be vigilant, always, to the possibility of money laundering/Terrorist Financing activities.
- Ensuring that his/her work complies with all applicable laws, and regulations on Anti-Money Laundering/Combating Terrorism Financing / Counter Proliferation Financing.
- Certifying to the Chief Compliance Officer on an annual basis that they have read the Anti-Money Laundering/Combating Terrorism Financing/Countering Proliferation Financing policy and aware of their AML legal obligations by signing the Annual Anti-

Money Laundering/Combating Terrorism Financing/Countering Proliferation Financing Compliance Attestation.

- Ensure complete KYC documentation and Customer Due Diligence (CDD)
- Report unusual transactions to the AML/CFT/CPF Compliance Unit.
- Maintain records – no document is a waste.
- Attend scheduled training.
- Promptly report to the Chief Compliance Officer all suspicious transactions or collusion in respect of money laundering activities.
- Being aware of their liability under the legislation should they fail to report information in accordance with internal procedures and legislation.
- Complying fully with all money laundering procedures in respect of customer identification, account monitoring, record keeping and reporting.
- Not tipping off any customer that a suspicious report has been made or their account is under investigation.

1.5.8. The Internal Audit

They will be responsible for (but shall not be limited to):

- Auditing compliance with the statutory and regulatory obligations to prevent money laundering and the financing of terrorist activities.
- Testing the effectiveness of the Bank's Anti-Money Laundering/Combating Terrorism Financing policies/Countering Proliferation Financing and program.
- Carrying out an annual review of the compliance function.
- Reporting cases of non-compliance by branches and departments to the Chief Compliance Officer.
- Investigate all reported cases of fraud and financial malpractice.

1.5.9. Human Resources

They are responsible for (but shall not be limited to):

- Verifying the identity of all employees and checking that they do not appear on any blacklist such as Office of Foreign Assets and Control, Central Bank of Nigeria, Nigeria Financial Intelligence Unit, Economic and Financial Crimes Commission, Bankers' Committee, or Internally Generated watch/Blacklist.
- Arranging in conjunction with the Chief Compliance Officer, formal training for all staff on Anti-money laundering as appropriate to their job functions in accordance with the Money Laundering laws and other relevant regulations.
- Ensuring that Money laundering subject is comprehensively covered in the training curricular at the bank's training centers.
- Ensuring that all newly engaged staff are trained on Anti-Money Laundering/Combating Terrorism Financing/Countering Proliferation Financing and undergo the AML/CFT/CPF training within six months of their employment.

1.5.10. IT Staff

Responsible for (but shall not be limited to):

- Ensuring that the systems used by the Bank to monitor, identify, investigate, and report suspicious transactions/activities function properly.
- Implementing the software for checking the names on watch lists.

1.5.11. Chief Risk Officer (CRO)

Responsible for (but shall not be limited to):

- Embed ML/TF/PF risks in the overall risk management framework of the Bank.
- Put in place ML/TF/PF risk classification system.

- Considering the ML/TF/PF risks in approving expansion of business e.g., new branches and new markets (domestic and foreign) products/ services.
- Stress tests the Enterprise Risk Management Framework via Risk and Control Self-Assessment of risk areas and document the mitigants.

Section 2: Overview of Money Laundering, Terrorism Financing and Proliferation Financing

2.1. Money Laundering

Money Laundering has been defined as the process of disguising the source and control of illegally obtained funds by making it appear as if the funds were legally obtained. The whole aim is to allow criminals access to these illegitimate funds, which have been derived from predicate offences, without having to pay the price for the crime committed. Some of the predicate offences include drug trafficking, fraud, smuggling, human trafficking, and tax evasion among others.

2.2. Stages of Money Laundering

The first step in the laundering process is for criminals to attempt to get the proceeds of their crimes into a bank or other financial institution, sometimes using a false identity or third parties. They can then transfer the proceeds to other accounts, here or abroad, or use the funds to buy other goods or services. It eventually becomes legally earned money and becomes difficult to trace to the crime. The criminals can then invest or spend it or as is often the case, use it to fund more crime.

The three steps below are the basic stages of money laundering:

Placement (Injection, or Pre-washing)

This is the stage where criminal funds are introduced into the financial system. To throw the Bank off the trail, the criminal may mix funds derived from illegitimate sources with funds derived legitimately. This is the most vulnerable stage for the money launderer as the funds are often still close to the source. As a result, banking transactions, involving cash are likely to take place in amounts under the Currency Transaction Report thresholds; this activity is called 'structuring.'

Furthermore, the use of false identities to conduct these transactions is common; banking officers should be vigilant in looking for false identification documents. To conceal their activities, money launderers will often result to 'smurfing' activities to get into a financial institution. 'Smurfing' is the process of using several individuals to deposit illicit cash proceeds into many accounts at one or several financial institutions in a single day.

Layering (Stacking or Washing)

The second stage concentrates on separation of proceeds from the criminal activity using various layers of monetary transactions. This is the creation of a complex web of financial transactions aimed at concealing the audit trail and separating money from its criminal origin. Generally, it seeks to hamper investigation, or wipe out audit trails, disguise origin of funds and maintain anonymity for people behind the transactions.

Integration (Recycling)

This is the point where the money launderer re-introduces the funds (origin properly disguised) into the economy with an aura of legitimacy, Examples include purchase of petrol stations, purchase of motor vehicles etc. At this point, it is often difficult to tell that the funds were illegally derived.

A money laundering cycle may or may not contain all the three steps above. However, it is pertinent to note that the Bank can be used to launder illegal funds at any of the stages.

2.3 Combating Terrorism Financing

Terrorist/Terrorism Financing

Terrorism can be defined as criminal acts intended or calculated to provoke a state of terror in the public by a group of persons or an individual for political purposes. This is considered terrorism regardless of the considerations of political, philosophical, ideological, racial, ethnic, and religious or any other nature that may be invoked to justify them.

Terrorist Financing refers to the act of providing funds to facilitate or sponsor terrorists and/or terrorism. The funds can be derived from both legal and illegal sources and there is the possibility that the provider/sponsor is unaware of the illegal use of the funds provided. Therefore, adequate due diligence processes that will include information regarding the source and use of funds are vital.

The detection and tracking of funds intended to finance or sponsor terrorism are often made more difficult when the funds are raised from legitimate sources.

Terrorists and their organizations need finance for a wide variety of purposes – recruitment, training, travel, materials, and protection. A successful terrorist organization, like any criminal organization, is one that can build and maintain an effective infrastructure. For this, it must develop sources of funding, either from criminal funds or from legitimately obtained income (including charitable donations) and then, finally, a way to ensure that the funds can be used to obtain the items needed to commit acts of terrorism.

Terrorists often control funds from a variety of sources around the world and employ increasingly sophisticated techniques to move those funds between jurisdictions. In doing so they require the services of skilled professionals such as bankers, accountants, and lawyers. Tracking, intercepting, and strangling the flow of funds is a vital element in the global effort against terrorism. The intelligence that can be gained into terrorist networks through the knowledge of their financial transactions and dealings is vital in protecting national and international security and upholding the integrity of national and international financial systems.

Terrorist groups are known to have well-established links with organized crimes. There will be considerable overlap between the movement of terrorist funds and the laundering of criminal assets. However, there are two major differences between the use of funds for terrorism and criminal funds:

- Often only small amounts are required to commit a terrorist atrocity, thus increasing the difficulty of tracking the funds.
- Terrorism can be funded from legitimately obtained income, including charitable donations and it will not be clear at what stage legitimate earnings become terrorist assets.

Premium Trust Bank's process shall include watch list filtering at the point of account opening and intermittently against a universal sanctions list that includes internationally known terrorists and the Bank's internal watch list.

This shall be done by conducting checks on the names of new customers, as well as regular checks on the names of existing customers, and potential customers against the names in the

database. If there is any name match, the bank is required to take reasonable and appropriate measures to verify and confirm the identity of its customer. Once confirmation has been obtained, we must take the following action immediately:

(a) Freeze the customer's funds or block the transaction (where applicable) if it is an existing customer.
(b) Reject the potential customer if the transaction has not commenced.
(c) Submit a suspicious transaction report to NFIU; and
(d) Inform the relevant regulatory authorities.

2.4. The Difference between Terrorist Financing and Money Laundering.

- While large transactions may be a red flag to indicate the possibility of money laundering, terrorist financing is often associated with smaller amounts.
- While the origins/sources of the funds associated with money laundering are always illegitimate, the funds associated with terrorist financing may be a mixture of both legitimate and illegitimate funds and in some instances, the source of the funds may be wholly legitimate.
- While the money launderer aims to give the funds a perception of legality, the result of terrorist financing is always illegal.

2.5. Proliferation/ Proliferation Financing

Proliferation is defined generally as the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling, or use of nuclear, chemical, or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations. It includes technology, goods, software, services, or expertise.

According to FATF definitions, "Proliferation financing" refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

2.6. Three Stages of Proliferation Financing

The stages are broken down below:

Program fundraising sources: A proliferating country raises financial resources for in-country costs.

Disguising the funds: The proliferating state moves assets into the international financial system, often involving a foreign exchange transaction, for trade purposes.

Materials and technology procurement: The proliferating state or its agents uses these resources for the procurement of materials and technology within the international financial system.

2.7. Comparison between Money laundering, Terrorist Financing and Proliferation Financing

	Money Laundering	Terrorist Financing	Proliferation Financing
Source of Funds	Internally from within criminal organizations	Internally from self-funding cells (centered on criminal activity)	Often state-sponsored programs but also through fundraising activities by non-state actors
Conduits	Favours formal financial system	Favours cash couriers or informal financial systems such as Hawala and currency exchange firms	A formal financial system is preferred up until the point of entry into the Proliferating countries, where the money is then taken out **in cash** in a neighbouring country and carried into the proliferating countries, Additionally, the use of Distributed Ledger Technology (DLT) has become a widely used mechanism to settle transactions in countries like North Korea
Detection Focus	Suspicious transactions such as deposits uncharacteristic of the customer's wealth or the expected activity	Suspicious relationships, such as wire transfers between seemingly unrelated parties	Individuals, entities, countries, goods and materials, activities
Transaction Amounts	Large amounts often structured to avoid reporting requirements	Small amounts are usually below reporting thresholds	Moderate amounts
Financial Activity	A complex web of transactions often involving shell or front companies, bearer shares, offshore secrecy havens	Varied methods including formal banking systems, informal value-transfer systems, smuggling of cash and valuables	Transactions look like normal commercial activity, structured to hide the connection to proliferator or proliferation activities
Money Trail	Circular – money eventually ends up with the person who generated it	Linear – money generated is used to propagate terrorist groups and activities	Linear – money is used to purchase goods and materials from brokers or manufacturers. The money can also move in the opposite direction (i.e., from the broker/ manufacturer to the proliferator).

2.8. Importance of Preventing and Detecting of Proliferation Financing

Proliferation financing facilitates the movement and development of proliferation-sensitive goods. The movement and development of such items can contribute to global instability and if proliferation-sensitive items are deployed, this may ultimately result in the loss of lives.

2.9. Difficulties Faced with Identifying Proliferation Financing.

There are several challenges associated with identifying proliferation financing:

- The identification and assessment of proliferation financing can be very complex thereby causing difficulties in detecting and reviewing the source of these funds.
- There is a growing trend in the purchase and sale of elementary components, as opposed to whole manufactured systems, for proliferation purposes. These are described as dual-use goods which are difficult to identify, requiring specialist knowledge of the item. These may also have perfectly legitimate uses making it challenging, at times, to ascertain the intention behind the use of those goods and whether they will be used for illicit purposes.
- The networks through which proliferation-sensitive goods may be obtained tend to be complex. Front companies, agents, and other intermediaries are often used to cover up the ultimate end-user. The lack of transparency and opaque processes allow for proliferation sensitive goods, the entities involved, the linked transactions and the ultimate end-user to avoid detection, significantly increasing the risk of proliferation financing.

2.10. Dual Use Goods

Dual-use goods are items that have both commercial and military or proliferation applications. These goods can be classified for civilian use and then transformed for military purposes, or worse, used for terrorism. In view of the potential use of converting dual use goods for terrorism purposes, there is need to monitor money laundering and other risks associated with trade financing businesses, including transport of dual-use and other restricted goods. Examples of qualifying dual use goods is tabulated below:

Centrifuges	Machine Tools	Heat Exchanges	Pressure Gauges
Scrubbers	Filters	Isostatic Presses	Precursors Tanks
Bacterial Strains	Aluminum Powders	Pulse Generators	Homing Devices
Accelerometers	Maraging Steel	Connectors Pumps	Ignition Pumps
High-speed Cameras	Elevators	Composites	Growth Media
Mixing Vessels	Mills	X-ray Flash Apparatus	Oxidants
Fermenters	Gyroscopes	Coolers	Vacuum Pumps
Aluminum Alloys	Mass Spectrometers	Spray Dryers	Reactors
Fertilizer	Condensers		

2.11. The Predicate Offences

Predicate offences may be described by reference to all offences, or to a threshold linked either to a category of serious offences or to the penalty of imprisonment applicable to the predicate offence (threshold approach), or to a list of predicate offences, or a combination of these approaches. Below are some of predicate offences:

a. Participation in an organized criminal group and racketeering
b. Terrorism, including terrorism financing.

c. Financing the proliferation of weapons of mass destruction
d. Trafficking in persons and migrant smugglings
e. Sexual exploitation, including sexual exploitation of children.
f. Illicit trafficking in narcotic drugs and psychotropic substances
g. Illicit arms trafficking
h. Illicit trafficking in stolen and other goods
i. Corruption
j. Bribery
k. Fraud
l. Currency counterfeiting
m. Counterfeiting and piracy of products
n. Environmental crime
o. Murder
p. Grievous bodily injury
q. Kidnapping, illegal restraint and hostage-taking
r. Robbery or theft
s. Smuggling includes smuggling in relation to customs and excise duties and taxes.
t. Tax crimes, related to direct taxes and indirect taxes.
u. Extortion
v. Forgery
w. Piracy
x. Insider trading and market manipulation or
y. Any other predicate offence under the MLPPA, TPPA, other relevant laws and regulations

2.12. Common Indicators of Money Laundering

a. Unexplainable and sudden wealth
b. Large amounts of cash
c. Irregular work/travel patterns
d. Suspicious banking
e. No apparent job but lots of money
f. Business not producing income.
g. Owning/investing in cash businesses
h. Use of nominees to purchase assets.
i. Excessive use of rented vehicles
j. Acquisition of vehicles
k. Others

2.13. Consequences of Money Laundering, Terrorist Financing and Proliferation Financing.

a. Unexplained, unusual, and rapid changes in supply and demand of money thereby causing diluted excess liquidity in the financial sector.
b. Volatility of capital flows and exchange rates due to un-anticipated cross border asset transfers.
c. Contamination of legal financial transactions
d. Prudential risks to bank soundness arising from these developments.
e. Non-compliant countries are blacklisted by FATF with attendant repercussions.
f. Facilitates institutional failures through reputational, operational, and legal risks.
g. Creates avenues for the perpetration of other crimes through transfer of economic power to criminals who possess the financial strength to buy up the economy.
h. Undermines development by diverting public funds for personal use.

i. Undermines confidence in public institutions such as the judiciary through subversion of justice and electoral process.
j. Undermines nation' s security.

2.14. Economic Consequences:

a. Rapid loss of investment/decline of grants & aids
b. Money Laundering/Terrorism Financing/Proliferation Financing may cause outflow of funds as investors lose confidence to invest in such economies.
c. Donors may decline assistance to affected countries.
d. Sudden inflows of illicit funds
e. Negatively impact the pricing regime for investment assets and other goods and services
f. Volatile exchange and interest rates
g. Posing a regulatory burden on legitimate cross border economic activities.

2.15. Social Consequences:

a. Money Laundering/Terrorism Financing/Proliferation of Weapons cause poor standard of living / infrastructural development.
b. Non provision of essential amenities/facilities because of corruption
c. Corruption in the award of government contracts could lead to provision of substandard goods & services and outright non execution of projects.
d. Attendant consequences include poverty and poor infrastructural development.
e. Escalates crimes such as murder and general insecurity as criminals jostle for control of proceeds and markets.

2.16. Political Consequences:

Adversely affects the development of democratic ideals and as such results in political instability.

2.17. Human Trafficking

Human trafficking is the criminal trade of men, women, and children for the purposes of commercial sex, forced labor, or other forms of exploitation. The potential to generate such sizeable financial returns makes money laundering and human trafficking go hand in hand.
Human trafficking takes numerous forms; however, its victims are normally recruited by coercion, fraud, or force and then exploited on an ongoing basis for profit. To exploit their victims, traffickers often move them between locations or across international borders.

The FATF identifies three categories of human trafficking:

Human trafficking for sexual exploitation

Victims forced into prostitution over an extended period. Traffickers often must meet the basic welfare needs of sexual exploitation victims, providing things like food, accommodation, and transport. In this type of trafficking, financial flows may be directed through victims or through the traffickers and money launderers themselves.

Human trafficking for forced labour

Victims are forced to provide free or extremely low-paid labour for traffickers in manual-labour roles, such as construction or farming. Victims of human trafficking are often recruited by traffickers with the incentive of better or higher-paid jobs overseas. After recruitment, victims are forced into work through violence and intimidation, the restriction of identity papers or threats of exposure to immigration officials. Some forms of forced labour are classified as modern slavery since the victims receive little to no payment in return for their work.

Human trafficking for the removal of organs
Victims are paid, coerced, or even tricked into having organs removed for the profit of traffickers. Human trafficking for organ removal often requires an elaborate logistical and financial infrastructure, involving multiple parties and even medical services. Though human trafficking for organ removal is a less common form of crime but nonetheless causes serious harm to its victims.

2.18. The Relationship Between Money Laundering and Human Trafficking
Perpetrators of human trafficking use money laundering to transform their financial proceeds into legitimate funds. However, because the financial flows from human trafficking are so diverse, detecting attempts to launder proceeds can be challenging.

Red-flag indicators for detecting human trafficking include:

- Large deposits of money into accounts which are then immediately withdrawn in towns close to international borders.
- Patterns of card transactions in even amounts of money between 10 pm and 6 am.
- Multiple victims sharing bank account information, e.g., phone number or address.
- Sudden deviations from expected customer account activity.
- Use of anonymous financial instruments to pay bills.
- Structured deposits across multiple physical banking locations.
- A single account is being used to pay wages to multiple employees.
- Wages are deposited into an account and then quickly withdrawn or transferred to a different account.

2.19. Legislations and Regulations on AML/CFT/CPF
Legal Framework- Local

- Money Laundering (Prevention and Prohibition) Act 2022
- Terrorism (Prevention and Prohibition) Act 2022
- Proceeds of Crime (Recovery and Management) Act 2022
- CBN AML/CFT/CPF Regulation 2022
- SEC AML/CFT/CPF Regulations, 2022
- Company and Allied Matter Act 2020
- Banking and Other Financial Institutions Act (BOFIA) 2020
- CBN AML/CFT/CPF (Administrative Sanctions) 2018
- Terrorism Prevention [Freezing of International Terrorist Funds and Other Related Measures] Regulations, 2013
- Economic and Financial Crimes Commission (Establishment) Act 2004
- National Drug Law Enforcement Act (NDLEA) 1989
- Failed Banks (Recovery of Debts) and Financial Malpractices in Banks Act 1994 (amended 1999)
- The Corrupt Practices and Other Related Offences Act (CPRO) 2000
- Securities Exchange Commission Act (SEC) 1997, (amended 2007)
- Nigerian Deposit Insurance Corporation Act (2006)
- Foreign Exchange Monitoring & Miscellaneous Act 1995
- National Insurance Commission Act (NAICOM)

Section 3. Anti-Money Laundering/Combating Terrorism Financing/Countering Proliferation Financing Program

To ensure an effective Anti-Money Laundering/Combating Terrorism Financing/Combating Proliferation Financing program, the Bank has put in place the following key pillars of compliance:

3.1. Designation of a Compliance Function

3.1.1. Process Owners

The process owners are the first line of defense in managing the Bank's Compliance risks. The Bank ensures the recruitment of the right people. The staff members are trained accordingly to enable them to understand, appreciate and handle basic compliance issues they encounter. The Bank has also clearly documented the Anti-Money Laundering/Combating Terrorism Financing and Countering Proliferation Financing policy and all other compliance policies and ensure that staff members clearly understand what is expected of them. Staff members shall be held accountable for their desks/roles.

3.1.2. Cluster Compliance Officers

These are designated Compliance Officers at various locations of the Bank with the responsibility of overseeing and conducting a second-level check of the branch's operational activities as it relates to money laundering, terrorist financing and proliferation financing control measures. The CCOs are the representatives of the Chief Compliance Officer in their clusters and must drive compliance with extant laws, regulations, and best practices. The CCO reports and escalates to the Chief Compliance Officer through the Head Office Compliance team.

3.1.3. Head Office Compliance Team

The Head Office Compliance Team is responsible for centrally coordinating, identifying, and addressing the Bank's compliance risks. The team can be reached via compliance@premiumtrustbank.com

3.2. Development of Internal Policies, Procedures, and Controls

The Bank has documented its Customer Identification and Acceptance policies. These policies, when read together, clearly stipulate the type and category of people the Bank is willing to take on as customers. It goes on to include the conditions under which it will deal with these persons/entities and the controls put in place to manage any attendant risk associated with the business.

3.3. Ongoing and Relevant Compliance Training of all Staff

The Bank shall ensure that all staff are trained adequately in Compliance.

- **Induction** – Compliance training shall form part of the curriculum for training new staff/intakes. At this point, the new intakes are sensitized on the Compliance culture of the Bank.
- **Refresher Courses** – Every existing member of staff shall undergo at least one compliance training in a year. To help drive this, the Bank has rolled out its Computer-Based Compliance training for all staff. This is an eLearning program at the end of which the staff will be tested.
- **Role Specific / Targeted Training** - From time to time, the Compliance Function, in conjunction with the relevant stakeholders, shall organize job-specific compliance training for designated units and job functions.
- **Compliance Notes** – The Compliance Function shall disseminate internal memos on topical compliance issues to sensitize staff members. New regulations shall also be

disseminated to the relevant units/staff members. Where the issue cuts across the Bank, this shall be circulated to all staff.

- Seminars and workshops with the active participation of the regulatory authorities.
- Knowledge sharing sessions within each branch/department.

3.3.1. Training Records

Records of training on Anti-Money Laundering/Combating Terrorism Financing and Countering Proliferation Financing provided to staff will be maintained to show the following:

- The persons trained
- The dates of the training
- The subject matter of the training
- The facilitators
- Annual Anti-Money Laundering/Combating Terrorism Financing/Countering Proliferation Financing training plan and budget.

3.3.2. All Staff

All employees must be aware of and understand the legal and regulatory environment in which they operate including relevant money laundering /terrorist financing/ proliferation financing prevention provisions, as well as measures to give effect to the bank's risk-based approach to Anti-Money Laundering. All staff will have a general understanding of the requirements of the relevant laws and regulations on Anti-Money Laundering/Combating Terrorism Financing and Countering Proliferation Financing regulations.

3.3.3. New Employees

All new employees would be given a general introduction to money laundering and the procedures for reporting suspicious transactions/activities before they become actively involved in day-to-day operations.

3.3.4. Operations/Marketing Staff

Employees who deal with the public such as tellers, marketing, relationship management, etc., are the first point of contact with potential money launderers, and their efforts are vital to the bank's effectiveness in combating money laundering. Staff responsible for opening new accounts or dealing with new customers should be aware of the need to obtain and verify the customer's identity, account monitoring procedures, and record retention period of the bank. Training would be given on customer acceptance and identification procedures, account opening and monitoring as well as factors, which may give rise to suspicion about a customer's activity, and procedures to be adopted when a transaction is considered suspicious.

3.3.5. Directors and General Management

Although Directors and members of General Management may not be involved in the day-to-day procedures for handling transactions that relate to money laundering, they must understand the statutory duties and responsibilities placed on them, their staff, and the Bank itself for preventing money laundering in the Bank. They would receive a higher level of training covering all aspects of money laundering laws, regulations, and procedures, including the offences and penalties arising from the relevant primary legislation for non-reporting or for assisting money launderers, and the requirements for verification of identity and retention of records.

3.3.6. Chief Compliance Officer (CCO)

The Chief Compliance Officer and other Compliance Officers would receive in-depth training on all aspects of the primary legislation, the regulations and internal policies and procedures on Anti-Money Laundering/Combating Terrorism Financing and Counter Proliferation Financing. They would also receive appropriate instructions on the determination and reporting of suspicious activities, on the feedback arrangements and on new trends of criminal activity.

3.4. Quality Assurance of the Compliance Function

3.4.1. Branch Reviews – The Cluster Compliance Function shall carry out periodic quality assurance on the branches. This will confirm the level of compliance in their respective clusters. This shall be in addition to the general bank-wide quality assurance provided for all the Bank's branches by the Internal Audit Team.

3.4.2. Internal Audit – The Bank's Internal Audit Team shall conduct a review of the Head Office Compliance Function at least once a year.

3.4.3. External Audit – The Audit of the Bank's Head Office Compliance Function shall form part of the bank-wide audit conducted by the Bank's External Auditors.

Section 4.0. Customer Due Diligence (CDD)

4.1. Definition of Customer

For KYC purposes, a 'Customer' is:

I. A person or entity that maintains an account and/or has a business relationship with the Bank.
II. One on whose behalf the account is maintained (i.e., the beneficial owner) – [Beneficial Owner means the natural person who ultimately owns or controls a client and or the person on whose behalf a transaction is being conducted and includes a person who exercises ultimate effective control over a juridical person].
III. Beneficiaries of transactions conducted by professional intermediaries, such as Stockbrokers, Chartered Accountants, Solicitors, etc. as permitted under the law, and.
IV. Any person or entity connected with a financial transaction can pose significant reputation or other risks to the bank, say, a wire transfer or issue of a high-value demand draft as a single transaction.

4.2. When CDD is compulsory

Financial institutions are required to undertake customer due diligence (CDD) measures when:

a. Business relationships are established.
b. Carrying out occasional transactions above the applicable designated threshold of $1,000.00 or its equivalent in other currencies or as may be determined by the CBN from time to time, including where the transaction is carried out in a single operation or several operations that appear to be linked and
c. Carrying out occasional transactions that are wire transfers, including those applicable to cross-border and domestic transfers between financial institutions and when credit or debit cards are used as a payment system to effect money transfer.
d. Any transfer flowing from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanying such transfers does flow from the transactions such as withdrawals from a bank account through an ATM, cash advances from a credit card or payment for goods.

e. Financial institution to financial institution transfers and settlements where both the originator-person and the beneficial-person are financial institutions acting on their own behalf.
f. There is a suspicion of money laundering or terrorist financing, regardless of any exemptions or any other thresholds referred to in this policy; or
g. There are doubts about the veracity or adequacy of previously obtained customer identification data.

4.3. Customer Due Diligence Measures (CDD)

Financial institutions are required to identify their customers (whether permanent or occasional; natural or legal persons; or legal arrangements) and verify the customers' identities using reliable, independently sourced documents, data, or information. All financial institutions are required to carry out the full range of the Customer Due Diligence measures in this policy. However, in reasonable circumstances, financial institutions can apply the Customer Due Diligence measures on a risk-sensitive basis.

In respect of customers (Ultimate Beneficial Owners) that are legal persons or legal arrangements, financial institutions are required:

- To verify any person purporting to have been authorized to act on behalf of such a customer by obtaining evidence of his/her identity and verifying the identity of such a person; and
- To verify the legal status of the legal person or legal arrangement by obtaining proof of incorporation from the Corporate Affairs Commission (CAC) or similar evidence of establishment or existence and any other relevant information.

- Financial institutions are required to identify a beneficial-owner and take reasonable measures to verify his/her identity using relevant information or data obtained from a reliable source to satisfy themselves that they know who the beneficial-owner is.
- Financial institutions are required to determine whether a customer is acting on behalf of another person. Where the customer is acting on behalf of another person, the FI is required to take reasonable steps to obtain sufficient identification data and to verify the identity of that other person.
- Financial institutions are required to take reasonable measures in respect of customers that are legal persons or legal arrangements to:

a. Understand the ownership and control structure of such a customer; and
b. Determine the natural persons that ultimately own or control the customer.
c. Natural people include those persons who exercise ultimate and effective control over the legal person or arrangement. The CBN AML/CFT/CPF Regulation 2022 Section 21 requires that the natural persons that are beneficial owners of corporate entities are unveiled to the minimum threshold of 5%. Due diligence shall be conducted on all legal persons and arrangements who own 5% shares or more in any legal entity and on all parent entities. Examples of types of measures needed to satisfactorily perform this function include:

    1. For companies - The natural persons are those who own the controlling interests and those who comprise the mind and management of the company; and
    2. For trusts – The natural persons are the settlor, the trustee and the person exercising effective control over the trust and the beneficiaries.

d. Where the customer or the owner of the controlling interest is a public company subject to regulatory disclosure requirements (i.e., a public company listed on a recognized stock exchange) it is not necessary to identify and verify the identity of the shareholders of such a public company.

e. Financial institutions are required to obtain information on the purpose and intended nature of the business relationship of their potential customers.
f. Financial institutions are required to conduct ongoing due diligence on the business relationship as stated by the customers above.
g. The ongoing due diligence above includes scrutinizing the transactions undertaken by the customer throughout the relationship period between the financial institution and customer to ensure that the transactions being conducted are consistent with the financial institution's knowledge of the customer, its business and risk profiles, and the source of funds (where necessary).
h. Financial Institutions are required to ensure that documents, data, or information collected under the Customer Due Diligence process are kept up-to-date and relevant by undertaking reviews of existing records, particularly the records in respect of high-risk business relationships or customer categories.

4.4. Customer Acceptance Policy

The following customer acceptance guidelines indicating the criteria for acceptance of customers shall be followed in Premium Trust Bank:

- No account shall be opened in an anonymous or fictitious name. The Bank shall not allow the opening of or keep any anonymous account or accounts in fictitious name(s) or account(s) on behalf of persons whose identity has not been disclosed or cannot be verified.
- Customers shall be accepted only after verifying their identity, as laid down in the customer identification procedure. Documentary requirements and other information shall be obtained in respect of different categories of customers depending on perceived risk and in line with the Bank's CDD/KYC framework and applicable regulatory requirements.
- Before opening a new account, necessary checks shall be conducted to ensure that the identity of the customer does not match any person with a known criminal background or with banned or sanctioned entities such as individual terrorists or terrorist organizations etc. The Banks' internal watch-list and World-check list shall be used for this purpose. No account will be opened for individuals'/entities subject to any of the sanction lists.
- No account shall be opened where the Bank is unable to apply appropriate customer due diligence measures i.e., the Bank is unable to verify the identity and/or obtain documents required as per the risk categorization due to non-cooperation of the customer or non-reliability of the data/information furnished to the Bank.
- No account shall be opened for a customer or business segment blacklisted by the Bank or by the Regulators
- Account will not be opened or operated for customers who refuse the disclosure of the beneficial ownership of the account.
- The Bank does not deal in any type of crypto-currency, or in a currency that is not recognized and accepted by the Central Bank of Nigeria.
- The Bank will not open accounts for shell companies.
- Circumstances, in which a customer is permitted to act on behalf of another person/entity, shall be spelt out in conformity with the established law and practice of banking as there could be occasions when an account is operated by a mandate holder or where an intermediary may open an account in a fiduciary capacity.

4.5. Customer Identification Policy

The Customer Identification Program is intended to enable the bank to form a reasonable belief that it knows the identity of each customer. As a rule, a business relationship with

Premium Trust Bank will not be established until the identity of a potential customer is satisfactorily established. Where a potential customer declines to provide any account initiation information, the relationship will not be established. Furthermore, if follow-up information is not forthcoming, any relationship already established will be terminated.

The Bank's account opening procedures which also specify the identification documents and information required from each customer are contained in the bank's Operations Policy Manual. The Bank's Customer Identification Policy, processes and procedures is highlighted as follows:

Customer Identification
Identity means a set of attributes such as names used, and date of birth that is peculiar to an individual. These are features which can uniquely identify a natural or legal person. In the case of a natural person, the date of birth is required as an important identifier in support of the name.

Customer identification requires identifying the customer and verifying his/her identity by using reliable, independent source documents, data, or information. The first requirement of Customer Identification Procedures (CIP) is to be satisfied that a prospective customer is who he/she claims to be.
Secondly, the requirement of CIP is to ensure that sufficient information is obtained on the identity and the purpose of the intended nature of the banking relationship. This would enable risk profiling of the customer and determine the expected or predictable pattern of transactions.

Sanctioned Screening
Every potential customer is screened on the screening solution to established whether he/she is a sanctioned entity or politically exposed.
The bank does not open account for a sanctioned individual or entity and where a customer is politically exposed, a senior management approval is put in place to open and operate the account.
The bank screens its customers continuously against the global watchlist, national sanctioned list and PEP list. The list maintained in the Soft AML Solution are UN, EU, OFAC, HMT, NSC, EFCC, Blacklisted BVN, Politically Exposed Person/ INEC list and other relevant list which it updates regularly.

Categorization of Identification
For report rendition, the different identification types have been categorized as below:

Valid Identification Documents
- National Driver's License
- International Passport
- National Identification Card (NIMC Card or Slip)
- Permanent Voter's Card

References
A person who seeks to reference a potential customer shall meet the following criteria:

- The referee's account must be active.
- The referee's account must be fully KYC compliant.
- The account must have been in operation with Premium Trust Bank for at least six months (for internal references). For external referees, the Bank must receive a positive response from the Bank in question.

- The referee must complete the reference form.

Address Verification

Address verification is an integral part of the Know Your Customer process. Where a branch has not been covered by the outsourced address verification program, on no account, should a staff carry out "armchair address verification". A visitation report will be signed by the Branch Management.

It is important to note that confirmation that the customer lives or is connected to the address is equally as important as confirming that the address exists. To this end, the address verification should confirm that the address exists and that the customer in question lives at or is connected to the address.

Timing of Verification

The Bank will verify the identity of customers and beneficial owners before or while establishing a business relationship or conducting transactions for them. The Bank may however complete the verification of the identity of the customer and beneficial owner following the establishment of the business relationship, only when:

- This can take place as soon as reasonably practicable.
- The money laundering risks can be managed effectively.
- There is no suspicion of money laundering, terrorism, and proliferation financing risks.

Where a customer is permitted to utilize the business relationship prior to verification, the Bank will adopt risk management procedures concerning the conditions under which this may occur. These procedures will include a set of measures such as a limitation of the number, types and/or number of transactions that can be performed and the monitoring of large or complex transactions being carried out outside the expected norm for that type of relationship.

4.6. Failure to Satisfactorily Complete Customer Due Diligence

Where the Bank is unable to conduct the necessary due diligence, it shall:

- Not open the account, commence business relations, or perform the transaction; and
- File a suspicious transaction to the regulators.

If the bank has already commenced the business relationship, it is required to terminate the business relationship and render suspicious transaction reports to the Nigeria Financial Intelligence Unit (NFIU) only.

4.7. Customer Risk Assessment

Customer Risk Assessment is the cornerstone of an effective Anti-Money Laundering/Combating Terrorism Financing and Countering Proliferation Financing program. Parameters of risk perception are clearly defined in terms of the nature of the business activity, products and services, citizenship, location of the customer and his clients, mode of payments, volume of turnover, social and financial status etc. to enable categorization of customers into low, medium, and high-risk categories. The nature and extent of due diligence to be carried out on a customer will depend on the risk classification e.g., normal due diligence will be carried out on all categories of customers, while enhanced due diligence will be conducted on high-risk customers.

The Bank shall ensure that it conducts risk assessment on all potential customers to determine the following:

- Risk level/rating to be assigned to the customer (Low, Medium or High Risk)

- Due diligence to be conducted (Customer Due Diligence or Enhanced Due Diligence)
- Risk Assessment Cycle (1 year - high-risk, 2 years - medium and 3 years low-risk).

The Bank's Customer Risk assessment shall be automated. Each customer's rating will be determined by a set of algorithms as programmed in the system. As soon as the information relating to a customer is populated, a risk rating will be assigned based on the set algorithms.

Premium Trust Bank will put in place systems, processes and controls using a risk-based approach to enable it to identify, monitor and manage money laundering, terrorist financing and proliferation financing using the following criteria:

1. Customer characteristics
2. Geography
3. Products and Services
4. Delivery channels
5. Other Risk variables

In each case, the criteria may be modified by other risk variables specific to any customer or transaction and may include but are not limited to:

a. Size of transaction
b. Length of relationship and regularity of contact
c. Familiarity with a jurisdiction
d. Nature/Line of business

Using these criteria and risk variables, customers will be classified into three risk categories namely High, Medium, and Low based on the money laundering risk that they pose. The risk categorization will determine the extent of Customer Due Diligence including customer identification, identity verification and any additional customer information as well as ongoing monitoring that is required for a customer, in a way that ensures that the bank focuses its efforts where it is needed and will have the most impact and minimizes the discomfiture to customers.

4.7.1 Risk Assessment Cycle –

The risk assessment cycle shall be as follows:

- High Risk Customer - 1 year cycle.
- Medium Risk Customers - 2 years cycle.
- Low Risk Customers - 3 years cycle.

In addition to the above, risk assessment can be triggered by an event. For example, if a customer's status changes, if the Bank realizes that it does not have sufficient information on a customer, if there is a change in existing regulation and where the customer's transactions are consistently in breach of his/her established profile with the Bank.

The Bank will take a risk-based approach to the rating of each customer, and this will in turn affect the level of KYC information collected, this would include not only the level of documentation held but also the number and content of additional checks performed over the Internet or by obtaining media information. These factors may alter the bank's perceived rating and the risk level altered accordingly.

4.7.2. Risk Classification/Rating of Customer

Low Risk Customer

Individuals and entities whose identities and sources of wealth can be easily identified and transactions in their accounts mostly conform to the known profile may be categorized as Low risk. Assessment of the risk factor indicates that the bank is less vulnerable and there is a low chance of ML/TF/PF occurring for clients in this category.

- Salaried employees
- People belonging to the lower economic strata of society.
- Quoted companies on the stock exchange.
- Regulatory and Statutory bodies, etc.

Medium Risk Customers

Customers that are likely to pose a higher-than-average risk to the Bank should be categorized as medium or high risk. For this category, the accounts can be opened face to face at any branch of Premium Trust Bank or by agents for enterprises or by the account holder. The assessment of the risk factor indicates that the bank is moderately vulnerable and there is a moderate chance of ML/TF/PF occurring for customers in this category.

High Risk Customers

The assessment of the risk factor indicates that the bank is highly vulnerable and there is a high chance of ML/TF/PF occurring for customers flagged as high risk.

These include the following:

- Trusts, charities, Non-Governmental Organizations, and organizations receiving donations.
- Companies having close family shareholding or beneficial ownership.
- Politically Exposed Persons (PEPs)
- Close relatives of PEPs and accounts of which a PEP is the ultimate beneficial owner.
- Those with dubious reputations as per available public information.
- Accounts of non-face-to-face customers, etc.
- Non-Resident Accounts.
- Designated Non-Financial Businesses and Professions (e.g., dealers in jewelry, real estate, mechanized farming, construction, hospitality, NGOs, etc.)
- Financially Exposed Persons (FEPs) – are persons in positions of authority in blue chip companies and large conglomerates. They include high-level executives with management or director positions in these companies and establishments.
- Government Departments
- Government owned companies
- Bureau De Change
- And any other companies or businesses as classified in the extant regulations.

For this category, enhanced due diligence is required which includes information on the customer's background, nature and location of the activity, country of origin, source of funds and client profile, etc. in addition to proper introduction and identification. Premium Trust Bank shall subject such accounts to enhanced monitoring on an ongoing basis.

The categorization of customers under risk perception is only illustrative and not exhaustive. The branches may categorize the customers according to the risk perceived by them while considering the above aspects. For instance, a salary class individual who is generally to be classified under low-risk category may be classified otherwise based on the perception of the Branch/Office and other factors that can be attributed to the said individual like where he is also a close relative of a Politically Exposed Person or is domiciled in a high-risk country.

Whenever there is a suspicion of money laundering or terrorist financing or when other factors give rise to a belief that the customer does not pose a low risk, branches should carry out full-scale Customer Due Diligence (CDD) before opening an account.

Whenever there are suspicions of money laundering or financing of activities relating to terrorism or proliferation or where there are doubts about the veracity of previously obtained customer identification data, branches should review the due diligence measures including verifying the identity of the client and obtaining information on the purpose and intended nature of the business relationship.

4.8 Money Laundering/Terrorist Financing/Proliferation Financing Risk Assessment Process
Understanding the ML/TF/PF risks is an essential part of developing and implementing an AML/CFT/CPF regime.

A risk assessment allows Premium Trust Bank to identify, assess and understand its ML/TF/PF risks, once these risks are properly understood, the Bank can apply the AML/CFT/CPF measures that correspond to the level of risk.
PremiumTrust Bank adopts risk-based approach that are commensurate with the specific risks of money laundering and terrorist financing. Higher money laundering risks demand stronger controls. However, all categories of risk — whether low, medium, or high must be mitigated by the application of applicable controls as provided in this policy such as verification of customer identification, Know Your Customer (KYC) policies, and so on.

The ensuing paragraphs provide a framework for identifying the degree of potential ML/TF risks associated with specific customers and transactions to ensure focused monitoring of those customers and transactions that potentially pose the greatest risks of ML/TF/PF.

4.8.1 Identifying Specific Risk Categories
Attempts to conduct illegal activities through the bank may come from many different sources throughout the system. Certain products, services, customers, and geographic locations in which the bank operates may be particularly vulnerable or may have been historically used by criminals for ML/TF/PF activities.

The following specific products, services, customers, entities, and geographic locations are identified as having ML/TF/PF risk to the bank.

Products and Services
In evaluating the ML/TF risk with respect to products and services, the following become relevant: "Does a particular product or service. new or current:

- Does the product allow for anonymity?
- Does the product disguise or conceal beneficial owner of the customer?
- Does the product disguise or conceal the customer's source of wealth or funds?
- Does the product allow payment to 3rd parties?
- Does the product commonly involve receipt or payment in cash?
- Is the product identified as presenting a higher ML/TF/PF risk in the AML/CFT/CPF Regulations?
- Does the product allow for movement of funds across borders?
- Is there any threshold for the value of the transactions that can be carried out through the product?
- Is there any threshold for the number of transactions that can be carried out through the product?
- Is non-face to face account opening permitted?

- Does the product allow non-face to face transactions?

These categories can include the following:

- Electronic fund payment services: electronic cash such as stored value cards, domestic and international funds transfers and third-party payment processor; remittance activity: automated clearing house (ACH) transactions, automated teller machines (ATMs): and Mobile Phones Financial Services.
- Electronic Banking.
- Foreign Exchange and funds transfers.
- Domestic and international private banking.
- Trust and asset management services.
- Monetary instruments
- Foreign correspondent accounts, such as Payable True Account and foreign currency denominated accounts.
- Trade finance or letters of credit
- Special use or concentration (suspense) accounts.
- Lending activities particularly loans secured by cash collateral and marketable securities.

Individual Customers and Entities

Certain customers and entities may pose specific risks depending on the nature of the business, the occupation of the customer, or the nature of anticipated transaction activity into their account, an assessment of the risk level of various types of clients such as individuals, listed companies, private companies, joint ventures, partnerships, financial institutions and others who want to establish a relationship with the bank should be conducted to determine and define the level of risk for each individual customer.

For instance, in the case of individual customers, those who have a history of involvement in criminal activities should receive the highest ratings.

Political figures or those in political organizations should score toward the top scale, higher than officials of multinational corporations. In the case of corporate customers, for example, when the bank is approached by a private company, the risk is higher than it would be with a larger corporation because the due diligence that can be conducted is more limited,

Access to a considerable amount of publicly available information could result in a lower risk than with a small company that is not listed and for which public information is not available.

The following list, though not exhaustive, indicates the customers and entities that are likely to pose a higher level of risk to the bank:

- Foreign financial institutions including banks and foreign money services providers such as bureau de change, currency exchanges, and money transmitters.
- Foreign corporations and domestic business entities, particularly offshore corporations such as domestic 'shell' companies, private investment companies (PICs) and international business corporations (IBCs) located in high-risk geographic locations and tax havens.
- Politically Exposed Persons (PEPs) as defined in this Policy,
- Non-resident aliens and accounts held by foreign individuals.

- Cash intensive businesses, including, for example, restaurants and fast-food businesses, liquor stores, large merchandise distributors, privately owned vending machines operators, car dealers, etc.
- Foreign and domestic Non-Governmental Organizations (NGOs) and charities.
- Professional service providers such as attorneys, accountants, or real estate brokers.
- Casinos,
- Travel agencies.
- Leather goods stores.
- Jewel, gem and precious metals dealers.
- Brokers/dealers in securities.
- Import/ export companies.
- Money Transfer Agent (MTA).

Minor Account

Accounts in this category shall be subject of continuous monitoring by both the business team and Compliance. The balance on this account shall be subjected to a maximum of N50million and where there's need to exceed this amount, the approval of the CCO must be obtained.

Geographic Locations

In assessing customers' jurisdiction risk, customer service officers and relationship managers must be aware of the vulnerability of jurisdiction where customers reside, some might be in countries with higher risk of ML/TF/PF.

When looking specifically at money laundering risk with respect to customers' location of business or residents, the following should be considered amongst other factors:

- Terrorism and sanctions lists published by governments and international organizations that include legal prohibitions and designations published by the United Kingdom's Financial Services Authority, U.S. Office of Foreign Assets Control, the U.S. Financial Crimes Enforcement Network, the European Union, World Bank, the United Nations Security Council Committee, The Central Bank of Nigeria (CBN) sanction list, etc.

- Whether the country is or has been on the Financial Action Task Force (FATF) list, whether it is a member of the FATF, whether it operates Anti-Money Laundering (AML) controls equivalent to international best practices or has deficient standards.

- The overall reputation of the countries in question, in some, cash may be a standard medium of exchange. Others may have politically unstable regimes and high levels of public or private sector corruption. Still others may be widely known to have internal drug production or to be in drug transit regions.

It should however be noted that geographic risk alone does not necessarily mean a customer or transaction's risk level is high or low. Cases should be evaluated individually when assessing the risks associated with doing business, such as opening accounts or facilitating transactions, in certain geographic locations, when in doubt, contact the CCO,

Conduct of Risk Assessment on Business/Branch Expansion

AML/CFT/CPF risk assessments shall be carried out for existing businesses and potential businesses and branch expansion. The AML/CFT/CPF risks associated with countries that the Bank may have business dealings with shall be determined using the most recent Basel AML Index scores and ranking. The Basel AML Index is an annual measure of the risk of money

laundering and terrorist financing of countries aggregating 14 indicators that deal with AML/CFT/CPF regulations, corruption, financial standards, political disclosure and rule of law into one overall risk score. The Basel AML Index is designed to indicate the vulnerabilities of money laundering and terrorist financing within a country. The most recent Basel AML Index scores and ranking shall be used to rate the countries.

The ML/TF/PF risk level of the Bank's branches as well as potential branch locations shall be assessed as a combination of the following:

- location risk
- categories of customers in the branch
- the branch's predominant transaction types

The Bank's branch operations structure is a major touch point by customers, it's cash intensive and each branch is directly connected to the entire network of branches online, real time. This therefore exposes the Bank to money laundering and terrorist financing risks no matter their location. In view of this, irrespective of the location of a branch, each branch will be rated as either medium risk or high risk. For the evaluation of the AML/CFT/CPF risk level of the Bank's business locations, the under listed factors shall be put into consideration:

I. Volume of cash-based transactions in relation to the average annual cash processed bank- wide.
II. Customer Categories: This depicts the ratio of high-risk customers in the branch to the total customers maintained by the branch.
III. Number of accounts flagged by the monitoring solution: The risk level of branches in relation to this will be measured by comparing the number of accounts domiciled in a branch flagged by the transactions monitoring to the total number of accounts flagged by bank-wide in the year under review.
IV. FX Transactions: This will be measured by the volume of inter-border transactions processed in the branch in comparison to the average volume of transactions processed bank wide.
V. Predominant products and services in the branch and geographic environment of the business location.
VI. Location peculiarities in terms terror activities / banditry / human and drug trafficking. These activities may however not be limited by location or distance but remains a major factor for business locations with proximity.

All the above factors may not be exhaustive but provides guidance for assessing AML/CFT/CPF risks for both existing and potential business locations and shall form the basis of recommendations by Compliance Department to Management. In addition, risk mitigants to manage inherent and residual risks shall be part of Compliance recommendations.

4.8.2. Analysis of Specific Risk Categories

The next stage of the risk assessment process is the analysis of data obtained during the risk identification stage to accurately assess ML/TF/PF risk more accurately. Evaluation and analysis of data pertaining to the bank's activities should be considered in relation both to Premium Trust Bank's Customer Identification Program (CIP) and to Customer Due Diligence (CDD) information.

For this Policy, analysis of customers' data and account profile should specifically consider, the following:

- Purpose of the account
- Actual or anticipated activity in the account (i.e., turnover)

- Nature of the customer's business
- Customer's location/ Source of funds
- Type of products or services a customer uses.
- Structure of business

Others include:

- Method of opening account.
- Identification used.
- Nationality.
- Customer address information.
- Residency status.
- Beneficial Owners.

Section 5. Know Your Customer (KYC)

KYC is the due diligence that financial institutions and other regulated companies must perform to identify their clients and ascertain relevant information before doing financial business with them.

A customer for the purpose of our KYC policy is defined as:

- A person or entity that maintains an account and/or has a business relationship with the Bank.
- One on whose behalf the account is maintained (i.e., the beneficiaries).
- Beneficiaries of transactions conducted by professional intermediaries (third party account) such as Lawyers, stockbrokers etc.
- Any person or entity connected with a financial transaction which can pose significant reputational or other risks to PREMIUM TRUST Bank Ltd. An example is a wire transfer or issue of high value demand draft as a single transaction.

Our approach to KYC is from a wider prudential, not just AML/CFT/CPF perspective.

Sound KYC procedures must be seen as a critical element in the effective management of banking risks. KYC Safeguards go beyond simple account opening and record-keeping and require banks to formulate a customer acceptance policy and a tiered customer identification programme that involves more extensive due diligence for higher risk accounts and includes proactive account monitoring for suspicions activities.

To this end, the Bank's KYC policies and procedures emphasize the following:

- Obtaining the necessary documents and information from customer as specified in the Bank's Operations Policy manual.
- Prohibition of opening numbered or anonymous accounts or accounts in fictitious or pseudo names.
- Minimum acceptable identification evidence for low risk and low value accounts.
- Independent verification of the legal status of incorporated entities and sole proprietorships with the Corporate Affairs Commission in writing.
- Screening of customer information against database of individuals and entities subject to sanction (watch-list check) at on-boarding stage and quarterly, customer database scan as required by the AML/CFT/CPF regulations.
- Adherence to the regulation on Targeted Financial Sanction
- Identifying the customer as well as the beneficial owners and verifying that customer's identity using reliable, independent source documents, data or information.

- Profiling of customers and risk rating such that transactions by our customers are predictable.
- Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.
- Customer information update whenever the need arises.
- Obligation to report to the regulatory authorities' suspicious transactions, which may ultimately have a bearing with ML/TF/PF activities.
- The Bank as a matter of policy does not transact business with "shell corporations" as described under the International Conventions.
- The bank applies each of the CDD measures below but may determine the extent of such measures on a risk sensitive basis depending on the type of customer, business relationship or transaction.

The measures to be taken shall be consistent with any guidelines issued by competent authorities. The bank shall perform enhanced due diligence for higher risk customers, businesses, relationships, or transactions including-

- Non-resident customers.
- Private banking customers.
- Legal persons or legal arrangements such as trusts that are personal-assets- holding vehicles.
- Companies that have nominee-shareholders or shares in bearer form.
- Politically Exposed Persons, cross border banking and business relationships among others.
- Charitable organizations, Non-Governmental Organization, Money Services Businesses, Casinos, dealers in precious stone and any other business activities or professional as may be described by regulatory, supervisory and competent authorities.

5.1 Account Opening Procedures

This section sets out the Customer Due Diligence (CDD) procedures and highlights information and documentation requirements for account opening with respect to various categories of customers/account type.

Staff are expected to conform with the bank policy on account opening and ensure appropriate documentation when establishing account relationship with customers.

Private Individuals' Resident in Nigeria Individual (Ordinary Accounts)

- Duly completed account opening form.
- Valid means of identification (ID) of signatory or person introducing another customer.
- Residence permit (for expatriates)
- Passport photographs.
- Birth certificate of a minor and 2 passport photographs of the trustee (applicable to savings account for children).
- Tax Identification Number (applicable to residents of Abuja).
- Proof of residence.
- Duly registered Power of Attorney, where an individual appoints another person to be a signatory to his personal account.
- Bank Verification Number.

Private Individual Not Resident in Nigeria

For these categories of customers who cannot make face-to- face contact, any of the following would suffice as evidence of the name of the customer:

- Notarized International passports,
- Notarized National identity cards. or
- Notarized International driver's license.

Reference numbers, date and country of issue should be obtained, and the information recorded in the customer's file as part of the identification evidence.

Separate evidence is required to be obtained with respect to the applicant's permanent residential address from the best available evidence, preferably a source. The address must be verifiable by way of a recorded description or other means, "P.O. Box number" alone should not be accepted as evidence of address.

The above should be verified through a reputable credit or financial institution in the applicant's home country or country of residence. However, particular care must be taken when relying on identification evidence provided from other countries, such evidence must be duly confirmed.

Salary Savings Account

- Duly completed account opening form,
- Letter of introduction from the company/appropriate authority (for
- Valid means of ID
- Proof of residence.
- Bank Verification Number.

Corporate Account

- Duly completed account opening form.
- CTC of Form CAC 2,
- CTC of Form CAC7
- Certificate of incorporation.
- CTC of Memorandum and Articles of Association.
- Tax identification Number (TIN).
- Valid means of 1D of each signatory and Directors.
- Residence Permit (foreigners).
- Passport photograph of each signatory.
- Nigeria Investment Promotion Commission (NIPC) certificate (for corporate entities incorporated in Nigeria with foreign ownership).
- Executed Board resolution.
- Current proof of residence /address.
- Bank Verification Number of Beneficial Owners, Signatories, Directors.
- CBN Licence for finance companies and international money transfer operators.

Enterprise Account

- Duly completed account opening form.
- Certificate of registration of business name.
- Form of application of registration of business name.
- Tax Identification Number (TIN).
- Passport photographs of each signatory.
- Valid means of 1D of each signatory.

- Current proof of residence/address.
- Residence permit (foreigners).
- Bank Verification Number of the Proprietors and Signatories.

Partnership Account

- Duly completed account opening form.
- Partnership resolution,
- Certificate of registration of business name.
- Form of application of registration of business name.
- Tax Identification Number (TLN).
- Letter of appointment as bankers.
- Residence Permit (foreigners).
- Valid means of ID of each signatory.
- Proof of address.
- Partnership deed or agreement.
- Passport photographs of each signatory.
- Bank Verification Number Partners.

Clubs/Societies/Association/Unincorporated Societies

- Duly completed account opening package.
- Constitution, rules and regulations.
- CTC of certificate of registration.
- Passport photograph for each signatory.
- Society /Club/ Association's resolution to open account.
- Form of identification for each signatory.
- Tax Identification Number (TIN).
- Residence permit (foreigners).
- Proof of address.
- Bank Verification Number of Signatories and Trustees.

Ministries: Parastatals and Other Government Bodies

- Duly completed account opening form,
- Copy of gazette or Act establishing the parastatal (if applicable)
- Board resolution authorizing the opening of the account (if incorporated or has a duly constituted Board).
- Copy of certificate of incorporation (if an incorporated parastatal).
- Copy of MEMART (if incorporated or has a duly constituted Board).
- Valid means of LD of each signatory.
- Authorization of Accountant General of the Federation/State or relevant Local Government Council.
- BVN of Signatories.

Bureau De Change (BDC)

- Duly completed account opening form.
- All documents for corporate accounts plus the following
- CBN Licence.
- Bank Verification Number of Directors and Signatories.

Executors/Administrators

- Duly completed account opening form.
- Passport photograph.
- Letter of Administration or Probate.
- Valid ID for each signatory.

- Current proof of residence/address for each signatory.
- Banker's confirmation and letter of indemnity
- Bank Verification Number.

NGOs and Multilateral Agencies

- Duly completed account opening form.
- Passport photograph for each signatory.
- Valid Id for each signatory.
- References (two) for each signatory.
- Valid LD for each signatory.
- Registration certificate (If applicable) T
- ax Identification Number (TIN)
- Passport photographs for each signatory.
- Proof of address.
- Copy of Rules/Constitution.
- Bank Verification Number of Signatories, Directors and Trustees Beneficial Owners.
- SCUML certificate where applicable.

Trustees

- Duly completed account opening form.
- Passport photograph for each signatory.
- Valid Id for each signatory.
- References (two) for each signatory,
- Registration certificate (If applicable),
- Proof of residence/ address.
- Deed of appointment as trustees,
- Executed Board resolution.
- Bank Verification Number of Signatories and Trustees

Religious Bodies/Organizations

- Duly completed account opening form.
- Certificate of registration
- Constitution.
- Letter of introduction of the signatories to the account.
- Valid means of identification of the signatories.
- Two (2) references.
- SCUML certificate
- Bank Verification Number of Signatories and Trustees

Embassies, Consulates & High Commissions of Foreign Countries.

- Duly completed account opening form.
- Letter of credence of the ambassador from the home country.
- Copy of current international passport of signatories,
- Letter of reference from the Ministry of External Affairs.
- Official document from home country establishing the authority of the embassy to open the account and how the account is to be operated.
- Bank Verification Number of Signatories.

Staff Accounts

- Two recent passport photographs.
- Valid ID.
- Bank Verification Number.

5.2 Customer Due Diligence Information Verification

The above listed customer due diligence information should be verified by at least one of the following methods:

- For established corporate entities - reviewing a copy of the latest report and accounts (audited, if available).
- Conducting an enquiry by a business information service. or an undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted.
- Undertaking a company search and/or other commercial enquiries to see that the institution has not been, or is not in the process of being dissolved, struck off, wound up or terminated.
- Utilizing an independent information verification process, such as accessing public and private databases.
- Obtaining satisfactory prior bank references.
- Physical visitation to the corporate entity place of business; and
- Contacting the corporate entity by telephone, mail, or e-mail.

5.3 Ultimate Beneficial Ownership (5% & Above Shareholding) - Register maintenance and frequency of update.

The Bank shall identify and take reasonable steps to verify the identity of a beneficial-owner, using relevant information or data obtained from a reliable source to satisfy itself that it knows who the beneficial owner is through methods including-

a. Legal Persons:
The account opening process for legal persons shall include Identifying and verifying the natural persons, where they exist that have ultimate control ownership interest in the legal person, taking into cognizance that the fact that ownership interest can be so diversified that there may be no natural persons (whether acting alone or with persons) exercising control of the legal person or arrangement through ownership.

For the purposes of beneficial ownership determination, shareholders with **"5% and above"** shareholding in the legal person shall be identified and verified.

Where there is no natural person who has control over the legal person through 5% and above shareholding, the bank shall identify and verify the natural persons that control the legal person or arrangement through other means or the key senior management officers.

b. Trust
For trusts, the bank shall identify and verify the identity of the settlor, the trustee, the protector where they exist, the beneficiaries or class of beneficiaries and any other natural person exercising effecting/ultimate control or ownership. Such accounts should be designated as high-risk during account opening and the transactions scrutinized for suspicious or unusual transactions.

5.3.1 Frequency of Update.
The UBO register shall be updated frequently as customers are being onboarded. A review of the register would be carried out monthly to accommodate changes in customers' UBO status.

5.4 Politically Exposed Persons

"Politically Exposed Persons" (PEPs) are individuals who are or have been entrusted with prominent public functions in any country and people or entities associated with them. For example, Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, members of royal families, important political party officials and any "close associate" of a senior political figure (local /foreign).

PEP also include persons who are or have been entrusted with a prominent function by an international organization, including members of senior management including directors, deputy directors and members of the board or equivalent functions other than middle ranking or more junior individuals.

Business relationships with family members or close associates of PEPs involve reputation risks like those with PEPs themselves.

A political figure: This includes any corporation, business, or other entity that has been formed by, or for the benefit of, a politician (local/foreign).

Immediate Family: The "immediate family" of a political figure typically includes the figure's parents, siblings, spouse, children, and in-laws.

Close Associate: A "close associate" of a political figure is a person who is widely publicly known to maintain an unusually close relationship with the political figure and includes a person who can conduct substantial domestic and international financial transactions on behalf of the political figure. Although close associates are more difficult for banks to identify, they include individuals who, due to the nature of their relationship with the PEP, can conduct significant domestic and international financial transactions on behalf of the PEP.

Examples of PEPs include, but are not limited to:

- Heads of state or government.
- Governors.
- Local government chairmen.
- Senior politicians.
- Senior government officials.
- Judicial or military officials.
- Senior executives of state-owned corporations.
- Important political party officials.
- Family members or close associates of PEPs; and
- Members of Royal Families.

What is the Risk in Doing Business with PEP?

Accepting and managing funds from corrupt PEPs can severely damage the Bank's own reputation and can undermine public confidence in the ethical standards of the bank, since such cases usually receive extensive media attention and strong political reaction.

In addition, the bank may be subject to costly information requests and seizure orders from law enforcement or judicial authorities (including international mutual assistance procedures in criminal matters) and could be liable to actions for damages by the state concerned or the victims of a regime. Under certain circumstances, the bank and/or its officers and employees themselves can be exposed to charges of money laundering, if they know or should have known that the funds stemmed from corruption or other serious crimes.

Where to Begin

As with most aspects of compliance, the place to begin is with a risk assessment. The bank conducts a risk assessment of its products /services, customers, and geographies where business is conducted. The outcome of this assessment forms the basis of a PEP/KYC compliance program.

PEP Risk Assessment

The Bank assesses the risks posed to its banking activities based on the scope of operations and the complexity of the bank's customer relationships. Management establishes a risk profile for each customer to be used in prioritizing oversight resources and for ongoing monitoring of relationship activities,

The following factors are considered when identifying risk characteristics of Politically Exposed Persons:

- Nature of the customer and the customer's business: The source of the customer's wealth, the nature of the customer's business and the extent to which the customer's business history presents an increased risk for money laundering and terrorist financing. This factor is considered for private banking accounts opened for PEPs.
- Purpose and activity: The size, purpose, types of accounts, products, and services involved in the relationship, and the anticipated activity of the account,
- Relationship: The nature and duration of the bank's relationship (including relationships with affiliates) with the private banking customer.
- Customer's corporate structure: Type of corporate structure.
- Location and jurisdiction: The location of the private banking customer's domicile and business (domestic or foreign). The review considers the extent to which the relevant jurisdiction is internationally recognized as presenting a greater risk for money laundering or conversely, is considered to have robust AML standards.
- Public information: Information known or reasonably available to the Bank about the private banking customer. The scope and depth of this review depends on the nature of this relationship and the risks involved.

Risk Minimization

a. Conducting detailed due diligence at the outset of the relationship and on an ongoing basis where they know or suspect that the business relationship is with a "politically exposed person", The Bank assesses the countries with which it has financial relationships.

b. Where the Bank has business in countries vulnerable to corruption, it would establish who the senior political figures in that country are and determine whether their customer has any connections with such individuals (for example if they are immediate family or close associates).

c. The bank is more vigilant where its customers are involved in those businesses which appear to be most vulnerable to corruption.

d. Every effort is made to establish the source of wealth (including the economic activity that created the wealth) as well as the source of funds involved in the relationship — again establishing that these are legitimate, both at the outset of the relationship and on an ongoing basis,

e. The development of a profile of expected activity on the business relationship to provide a basis for future monitoring. The profile would be regularly reviewed and updated.

f. A review at senior management or board level of the decision to commence the business relationship and regular review, on at least once a year basis from the inception of the relationship.

g. Scrutiny of any unusual features such as very large transactions, the use of government or central bank accounts, particular demands for secrecy, the use of cash or bearer bonds or other instruments which break an audit trail, and regular transactions involving sums just below a typical reporting amount.

h. Full documentation of the information collected in line with the above. If the risks are understood and properly addressed, then the acceptance

The Bank's Obligations and Position on PEP accounts

Before any account is opened for any PEP, Senior Management approval must be obtained. For this purpose, Senior Management approval must be obtained from the line Chief Business Officer, Regional or Executive Director and the Chief Compliance Officer. This will be done as part of account opening formalities. No account would be opened for any PEP without the approval being in place.

The customers due diligence efforts do not end at account opening: ongoing account monitoring is expected. Activities on PEP accounts will be reviewed on transactions related to them and filing, as appropriate, STRs related to them.

Monthly returns will be sent to the CBN and NFIU on PEP transactions.

This is to assist the regulators in monitoring the activities of PEPs.

The Bank will take reasonable steps to ascertain the source of wealth and the source of funds of PEPs and report all anomalies to the CBN and other relevant authorities.

Periodic Enhanced Due Diligence and monitoring must be carried out on all PEPS by the Relationship Manager and or Account Officer concerned. On an annual basis, the relationship managers shall certify that none of the accounts reporting to them became PEP in the year. If any transaction is noted to be abnormal. such must be immediately flagged and reported to the Compliance Department immediately.

While circumstances will vary, certain transactions by PEPs are considered potentially suspicious and may be indicative of illegal activity.

The following guidance — provide a non-exhaustive list of red flags that includes, among other things:

- Requests to establish relationships with or route transactions through an institution that is unaccustomed to doing business with foreign people and that has not sought out business of that type.
- A request to associate any form of secrecy with a transaction, such as booking the transaction in the name of another person or business entity.
- The routing of a transaction through several jurisdictions without any apparent purpose other than to disguise the nature, source, or ownership of funds.

- The rapid increase or decrease in the funds or asset value in an account that is not attributable to market conditions.
- Frequent or excessive use of funds transfer or wire transfer either into or out of an account,
- Large currency or bearer instrument transactions in or out of an account.
- The frequent minimal balance or zeroing out of an account for purposes other than maximizing the value of the funds held in the account.

5.5 Designated Non-Financial Businesses and Professions (DNFBPS)

Financial institutions are required, prior to establishing business relationship with Designated Non-financial Businesses and Professionals. to obtain evidence of registration (e.g., certificate of registration showing registration number) with the Special Control Unit on Money Laundering (SCUML).

DNFBPs refer to dealers in jewelries, precious metals and precious stones, goods, audit firms, tax consultants, clearing and settlement companies, lawyers, notaries, other independent legal practitioners and chartered accountants, trusts and company service providers, hotels, casinos, supermarkets, real estate agents, non-governmental organization, religious and charitable organization etc.

The above DNFBPs customers include sole practitioners, partners and employed professionals within professional firms. They do not refer to "internal" professionals that are employees of other types of businesses nor to professionals working for government agencies who may already be subject to AML/CFT/CPF measures.

5.6 Correspondent Banking Relationship

The bank shall ensure that Correspondent-banking relationships are carefully selected. The bank shall not establish correspondent relationships with high-risk foreign banks, including shell banks with no physical presence in any country or with correspondent banks that permit their accounts to be used by such banks.

Executive management approval is mandatory for all correspondent bank relationships and on-going due diligence.

Compliance Department shall annually obtain the current list of the Bank's executive management approved correspondent bank relationships, review their AML/CFT/CPF framework, conduct adverse media search and other due diligence searches on their Board members as well as management, document the report for regulatory examination and take other appropriate action on negative findings.

5.7 Safe Custody

Precautions should be taken in relation to requests to hold boxes, parcels, and sealed envelopes in a safe custody, where such facilities are made available to non-account holders, the identification procedures, depending on the type of individual involved are followed.

5.8 Foreign Account Tax Compliance Act (FATCA)

The main objective of the Act is to counter offshore tax avoidance by US persons with money invested outside the US and ensuring that US persons with financial asset outside the US are paying the correct amount of US lax, e.g., US persons living outside the US, US persons hiding behind non-US companies, etc.

FATCA regime is to be administered by US financial institutions and **Foreign (non-US) Financial Institutions (FFIs)**

FATCA regulations incorporate a targeted risk-based approach aimed at:

- Maintaining the policy objective on reporting a US taxpayer within jurisdictions of information assets invested in non-US jurisdictions.
- Limiting the scope of entities, obligations and accounts affected by FATCA.
- Reducing due diligence and compliance burdens,
- Aligning with FATCA Intergovernmental Agreements (IGAs).

Refusal by a FFI to comply may result in application of 30% withholding tax on:

- US sourced fixed or determinable annual or periodic (FDAP) income payments made to the FFI.
- US sourced gross proceeds received by the FFI.

Refusal by a participating FFI's account holders to comply with information and reporting requests may result in the FFI having to apply 30% withholding tax on with-holdable payments made to their account holders.

FFIs may mitigate adverse FATCA compliance issues e.g., obtaining, deemed compliant status, or qualifying for exemptions under FATCA or IGAs.

5.9 Three Tiered KYC

Premium Trust Bank as a responsive institution fully supports CBN initiatives and has put measures in place to achieve the financial inclusion that this initiative is meant to achieve. The Bank utilizes flexible account opening requirements for low value and medium value accounts which are subject to caps and restrictions as the amount of transactions increase,

Features of Low-Valued (Tier 1) Accounts:

- They are strictly savings accounts.
- It allows maximum single deposit amount of N50,000.00
- It allows maximum cumulative balance of N300,000.00 at any point in time.
- The basic information required for the account opening are name, place/date of birth, photograph, gender, address, and telephone number.
- Mobile banking products, e-channels, and issuance of ATM cards are allowed.
- Mobile banking allowed subject to a maximum transaction limit of N3,000 daily limit of N30,000.00

Features of Medium-Valued (Tier 2) Accounts:

- They are strictly savings accounts,
- It allows maximum single deposit of N100,000,00
- It allows maximum cumulative balance of N500,000.00 at any point in time.
- The basic information required for the account opening are valid means of ID, name, place/date of birth, photograph, gender, address and telephone number.
- Address verification is a requirement.
- The customer information for account opening may be sent on-line (electronically)
- Allows for the use of mobile banking products, e-channels and issuance of ATM cards to customers.
- Mobile banking allowed subject to a maximum transaction limit of N10,000 daily limit of N100,000.00

Characteristics of High-Valued (Tier 3) Accounts:

- It has both savings and current account features.
- The Bank is required to obtain full account opening documentation requirement in line with the CBN AML/CFT/CPF Regulations, 2022

5.10. New Technologies and Non-Face-To-Face Transactions

Premium Trust Bank will pay special attention to any ML/TF/PF threats that may arise from new or developing technologies including credit/debit cards, mobile telephone banking, and internet banking, and take measures to prevent misuse of the technological developments in money laundering, terrorist financing or proliferation financing schemes. The Bank will apply effective customer identification procedures and ongoing monitoring standards to customers availing themselves of these new technology-driven products. It will put in place measures to address any specific risks associated with non-face-to-face business relationships or transactions before the launch of new products and services. The Bank will undertake the risk assessment before the launch or use of such products, services, and technologies. Appropriate measures will be taken to manage and mitigate the ML/TF/PF risks.

5.11. Financial Technology Companies

Financial technology companies, also known as Fintech, are institutions that employ the use of technology and innovation in the delivery of financial services. The innovations and technology used by these companies seek to improve the traditional financial methods of delivery of financial services. Premium Trust Bank shall observe due diligence in dealing with this category of customers to ensure that the company meets legal and regulatory requirements. The Due Diligence process shall include:

a. The unveiling of the company's ownership and governance structure
b. Screening of shareholders and directors against sanction lists/watchlist
c. The availability of the relevant regulatory license
d. Ascertaining the existence of AML/CFT/CPF policy within the company
e. Confirming the adherence to the Nigeria Data Protection Regulation (NDPR) by the company
f. Ongoing and continuous monitoring of transactions after on-boarding

5.12. Agency Banking

PremiumTrust Bank shall maintain effective oversight of the agent's activities and ensure that appropriate controls are incorporated into its system to ensure compliance with relevant regulations. The Bank shall include a risk-based review of critical agent banking processes to ensure that the policies, rules, regulations, and operational guidelines are adhered to.

Agents shall be trained on anti-money laundering (AML), combating financing of terrorism (CFT) and counter proliferation financing (CPF) requirements and report all suspicious activities/transactions.

In the fulfilment of AML/CFT/CPF requirements, the Bank shall ensure that Agents comply with the requirements as stated in the guidelines for the regulation of agent banking and agent banking relationships in Nigeria.

An agent shall not–

- Accept any withdrawals by cheque; or be a direct member of the Nigeria Bankers Clearing System; or
- Accept any deposit above an amount, which shall be prescribed, from time to time, by the Central Bank of Nigeria.

5.13. Customer Exiting Policy

In some circumstances, the Bank may be required to or choose to terminate its relationship with a customer. This policy seeks to clearly state the step-by-step approach to be adopted by Premium Trust Bank before informing a customer of the decision to terminate the relationship, how to notify the customer of the decision to terminate the said business relationship and what the Bank can do to ensure that the same customer does not open another account in a different branch of Premium Trust Bank.

- Instances, where the Bank may choose to terminate a relationship include where it is proven that the customer has carried out a suspicious transaction, the account has been used to perpetrate fraud, the customer fails or refuses to complete the Know Your Customer (KYC) process by providing the required information or the customer is found to be on any sanctioned list.

The process to terminate the relationship shall be as below:

a. The transaction or activity must immediately be reported to the Head Office Compliance Team.
b. The team reviews the case and obtains the requisite approval to file a Suspicious Transaction Report (where this has been determined to be necessary).
c. This is escalated to the Chief Compliance Officer who decides whether to exit or not to exit the customer.

Section 6. Record Keeping and Retention Requirements

6.1. Retention of Records

AML/CFT/CPF Regulations require financial institutions to maintain adequate records which are appropriate to the nature of the business, and which can be used as evidence in any subsequent investigation,

6.2. Why Retain Records?

Records must be retained, not only because regulations demand record retention but also to ensure that:

- Any legislation and KYC rules are met.
- Third parties, i.e., external auditors, can assess the effectiveness of the Bank's observation of AML/CFT/CPF procedures.
- Any transactions affected by the Bank on behalf of any customer can be reconstructed.
- Any customer can be properly identified and located.
- All suspicious reports, both internal and external, can be identified.
- The Bank can satisfy any enquiries or court orders from appropriate authorities.

6.3. For How Long Must Records Be Retained?

Section 8 of Money Laundering (Prevention and Prohibition) Act, 2022 states that:

A Financial Institution shall:

- preserve and keep records of a customer's identification of a customer for a period of at least five (5) years after the closure of the accounts or the severance of relations with the customer.
- Preserve and keep records and related information of a transaction carried out by a customer and the report provided for in section 4 and 9 of the Act for a period of at least five (5) years after carrying out the transaction or making of the report.
- The bank shall maintain all necessary records of transactions, both domestic and international, for at least five years after completion of the transaction or such longer

period as may be required by the CBN or NFTU. (For more details see the Bank's Records Management Policy).

- Records of all suspicious transactions shall be kept for the same period.

Section 7.0. Requests for AML/CFT/CPF Records by Regulator & Law Enforcement Agencies

Premium Trust Bank shall fully cooperate with regulatory/law enforcement agencies during their investigations and promptly respond to any requests for information in accordance with applicable laws.

Regulatory Requests / Letters

- Requests/Letters received by a branch from any regulator or Law Enforcement Agent shall immediately be scanned and sent to the Head Office Compliance via compliance@premiumtrustbank.com for further directive.
- The court/Banker's order attached to a request shall be confirmed or verified from the issuing court by the Branch to ascertain its genuineness before onward delivery to the compliance team.
- Compliance shall confirm that relevant authorization is in place (e.g., Court Order or any other statutory empowerment) and advise the branch or responsible unit to place lien, block, place memo, unblock, remove memo or lien accordingly.
- On no account should a branch respond to a regulatory letter or request on their own without the directive of the Head Office Compliance Team. Where the Law Enforcement Agent or regulator insists on getting an immediate response, they should be politely informed that such responses are centralized at Head Office. The branch shall immediately call Head Office Compliance for further directives.

Staff Invitation by Regulators

- All staff invitations shall be routed through the Head Office Compliance Team. Where a member of staff receives an invitation directly, this shall be forwarded to the Head Office Compliance team for further directive.
- No staff of the Bank shall honour an invitation from any Law Enforcement Agency or Regulator alone. Two Bank representatives one of which shall be from the Legal team and the other from the security office must accompany staff.
- As much as possible, a meeting shall be held with the staff in question and the Bank's representative to ensure that the staff is adequately prepared for the invitation.
- A report as to what transpired at the meeting with the regulator/Law Enforcement Agent shall be sent to the Head Office Compliance Team within 48hours of the visit.

Section 8.0 Reporting Suspicious Transactions

"Suspicious activity" is a difficult concept to define because it can vary from one transaction to another based upon all the circumstances surrounding the transaction.

Monitoring and reporting of suspicious transactions is key to AML/CFT/CPF effectiveness and compliance.

A suspicious transaction could be defined as one which is unusual because of its size, volume, type or pattern or otherwise suggestive of known money laundering patterns. It includes such transactions that is inconsistent with a customer's known, legitimate business or personal activities or normal business for that type of account or that lacks an obvious economic rationale. In this case, the Bank shall file STR to the relevant Regulatory authorities.

Unusual Transaction on the other hand may also be considered in relation to the size, volume and other deviation from the previous trend or pattern of transactions on the customer account which may cause an account being placed on Post No Debit (PND) pending the outcome of the investigation. In this case, STR shall not be filed with the relevant Regulatory Authorities, but instead, the Anti-money laundering and Compliance Staff shall file documents related to the transaction appropriately.

Premium Trust Bank shall treat a transaction as being suspicious, whether or not it relates to the laundering of the proceeds of a crime or an illegal act if it meets any of the criteria below or if in the opinion of the processing officer: involves a frequency which is unjustifiable or unreasonable surrounded by conditions of unjustified complexity, or appears to have no economic justification or lawful objective the authorized Officers is convinced that it is suspicious

A transaction by one customer may be normal because of the knowledge about that customer while similar transactions by another customer may be suspicious.

In Premium Trust Bank, the following additional factors shall be considered when determining whether a particular transaction is suspicious:

- The amount involved.
- Type of and destination of transactions
- Source of funds and actual beneficiary of the transactions
- Significant transactions relative to a relationship and transactions that exceed certain limits.
- Very high account turnover inconsistent with the size of the business
- Transactions which fall out of the regular pattern of the account's activity.

The Chief Compliance Officer shall supervise the monitoring and reporting of suspicious transactions.

The Chief Compliance Officer shall provide awareness programme to fully intimate both Directors, Staff and Management of the Bank of the various patterns of conduct that have been known to be suggestive of money laundering/terrorist financing and proliferation financing and maintain a checklist of such transactions.

8.1 Procedure for Suspicious, Doubtful or Unusual Transactions

When a transaction falls within the definition covered by this AML/CFT/CPF Policy, the authorized Staff of the branch where the transactions occur shall immediately follow the procedure below:

- Seek information from the customer as to the source of the funds, the purpose of the transaction and the identity of the beneficiary.
- The branch staff shall make a formal report to the AML/CFT/CPF Compliance immediately of the occurrence of the suspicious transaction.
- Upon receipt of the report, the AML/CFT/CPF Compliance shall carry out a careful check on the transaction to enable it to form an opinion whether it falls within the definition given above.
- The Compliance Team shall promptly review account/transactions under the supervision of the Chief Compliance Officer.

Once this is established, the Compliance Team shall draw up a written report containing all relevant information on the matter and forward to the Nigerian Financial Intelligence Unit

[NFIU] Suspicious Transaction Report (STR) immediately but not later than 24 hours of its occurrence.

8.2 Other Provisions on Suspicious Transactions

All suspicious transactions, including attempted transactions shall be reported regardless of the amount involved. This requirement applies regardless of whether the transactions involve tax matters or other things.

The Executive Compliance Officer (ECO) and Chief Compliance Officer (CCO) shall take other appropriate action to prevent further laundering of the proceeds of money laundering activities. Only the CCO shall be responsible for submitting the STR.

The Banks' Director, Management, Staff, and other utility employees (permanent and temporary) shall be prohibited from disclosing to the customer that a report shall be filed or has been filed with the competent authorities.

All Staff shall be trained in monitoring of unusual or suspicious transaction/activity based on the relevant criteria applicable in the jurisdiction where the Bank operates.

Foreign and Local Transactions are screened using the SWIFT screenings application to identify the sender and beneficiary, including their geographical locations and the eligibility of the transaction.

8.3 Procedure for Dealing with Customer after Reporting.

The branch shall report suspicious transaction to Head Office and shall not alert the customer that suspicion has been reported. **Tipping off is criminal.**

8.4 Staff Personal Responsibility for Suspicious Transactions

Once an employee becomes suspicious or ought to reasonably be suspicious of a customer's transaction or series of transactions, a report must be submitted immediately.

There shall be no assumption that someone else will submit a report because the staff will be held personally responsible, especially if he is the one who processed the transaction or had other dealings with the customer.

Staff who report a suspicious transaction shall be rewarded.

8.5 Maintenance of Record on Suspicious Transactions

The report on the findings above shall be kept for at least five years (electronic / hard copy) within which same could be made readily available in time of need.

8.6 Prohibition against Disclosing Suspicious Transaction Report (STR)

Premium Trust Bank shall maintain confidentiality in respect of such investigation and any suspicious transaction report that has been filed with the competent authority. Employees shall not alert a client or his representative(s) about suspicious transactions/dealings or about which an STR is underway for reporting to the Compliance Team. All STRs and any other supporting documentation shall be maintained as confidential, any staff that contravenes this is liable to a fine of N500,000. The staff is also at the risk of being prosecuted by law enforcement agents and liable on conviction to a fine of at least N10,000,000 or imprisonment for a term of at least two years.

The understanding of customer's identity vis-à-vis his stated norms of dealings, services, etc shall also have a bearing on transactions before they are viewed as suspicious transactions.

8.7 Money Laundering, Terrorism Financing and Proliferation Financing "Red Flags"
Transactions or activities highlighted in the list of suspicious transaction typologies are not necessarily indicative of actual ML/TF/PF if they are consistent with a customer's legitimate business.

The list of transactions and activities provided below is intended to understand mainly about the means and basic ways of money laundering process.

The list is by no means exhaustive. It shall be constantly updated and adapted to changing circumstances as new methods of money laundering and terrorism financing evolve.

A. Potential Transactions Perceived or Identified as Suspicious

- Transactions involving high-risk countries vulnerable to money laundering, subject to this being confirmed.
- Transactions involving shell companies.
- Transactions with correspondents that have been identified as higher risk.
- Large transaction activity involving monetary instruments such as traveler's cheques, bank drafts, money order, particularly those that are serially numbered.
- Transaction activity involving amounts that are just below the stipulated reporting threshold or enquiries that appear to test an institution's own internal monitoring threshold or controls.

ii. Money Laundering Using Cash Transactions

- Significant increases in cash deposits of an individual or corporate entity without apparent cause, particularly if such deposits are subsequently transferred within a short period out of the account to a destination not normally associated with the customer.
- Unusually large cash deposits made by an individual or a corporate entity whose normal business is transacted by cheques and other non-cash instruments.
- Frequent exchange of cash into other currencies
- Customers who deposit cash through many deposits slips such that the amount of each deposit is relatively small, the overall total is quite significant.
- Customers whose deposits contain forged currency notes or instruments.
- Customers who regularly deposit cash to cover applications for bank drafts.
- Customers making large and frequent cash deposits but with cheques always drawn in favour of persons not usually associated with their type of business.
- Customers who request to exchange large quantities of low denomination banknotes for those of higher denominations.
- Branches of banks that tend to have far more cash transactions than usual, even after allowing for seasonal factors.
- Customers transferring large sums of money to or from overseas locations with instructions for payment in cash.

C. Money Laundering Using Deposit Accounts
The following transactions may indicate possible money laundering, especially if they are inconsistent with a customer's legitimate business:

- Minimal, vague, or fictitious information provided by a customer that the deposit money bank is not in a position to verify.
- Lack of reference or identification in support of an account opening application by a person who is unable or unwilling to provide the required documentation.
- A prospective customer does not have a local residential or business address and there is no apparent legitimate reason for opening a bank account.

- Customers maintaining multiple accounts at a bank or different banks for no apparent legitimate reason or business rationale. The accounts may be in the same names or have different signatories.
- Customers depositing or withdrawing large amounts of cash with no apparent business source or in a manner inconsistent with the nature and volume of the business.
- Accounts with large volumes of activity but low balances or frequently overdrawn positions.
- Customers making large deposits and maintaining large balances with no apparent rationale.
- Customers who make numerous deposits into accounts and soon thereafter request for electronic transfers or cash movement from those accounts to other accounts, perhaps in other countries, leaving only small balances.
- Typically, these transactions are not consistent with the customers' legitimate business needs.
- Sudden and unexpected increase in account activity or balance arising from deposit of cash and non-cash items. Typically, such an account is opened with a small amount which subsequently increases rapidly and significantly.
- Accounts that are used as temporary repositories for funds that are subsequently transferred outside the bank to foreign accounts. Such accounts often have low activity.
- Customer requests for early redemption of certificates of deposit or other investment soon after the purchase, with the customer being willing to suffer loss of interest or incur penalties for premature realization of investment.
- Customer requests for disbursement of the proceeds of certificates of deposit or other investments by multiple cheques, each below the stipulated reporting threshold.
- Retail businesses which deposit many cheques into their accounts but with little or no withdrawals to meet daily business needs.
- Frequent deposits of large amounts of currency, wrapped in currency straps that have been stamped by other banks.
- Substantial cash deposits by professional customers into client, trust or escrow accounts.
- Customers who appear to have accounts with several institutions within the same locality, especially when the institution is aware of a regular consolidation process from such accounts prior to a request for onward transmission of the funds.
- Large cash withdrawals from a previously dormant/inactive account, or from an account which has just received an unexpected large credit from abroad.
- Frequent use of safe deposit facilities by individuals, particularly the use of sealed packets which are deposited and soon withdrawn.
- Substantial increase in deposits of cash or negotiable instruments by a professional firm or company, using client accounts or in-house company or trust accounts, especially if the deposits are promptly transferred between other client company and trust accounts.
- Large number of individuals making payments into the same account without an adequate explanation
- High velocity of funds that reflects the large volume of money flowing through an account.
- An account opened in the name of a money changer that receives deposits.
- An account operated in the name of an offshore company with structured movement of funds.

D. Trade-Based Money Laundering

- Over and under-invoicing of goods and services
- Multiple invoicing of goods and services.

- Falsely described goods and services and "phantom" shipments whereby the exporter does not ship any goods at all after payments had been made, particularly under confirmed letters of credit.
- Transfer pricing.
- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- Items shipped are inconsistent with the nature of the customer's normal business and the transaction lacks an obvious economic rationale.
- Customer requests payment of proceeds to an unrelated third party.
- Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.

E. Lending Activity

- Customers who repay problem loans unexpectedly
- A customer who is reluctant or refuses to state the purpose of a loan or the source of repayment or provides a questionable purpose and/or source of repayment.
- Loans secured by pledged assets held by third parties unrelated to the borrower.
- Loans secured by deposits or other readily marketable assets, such as securities, particularly when owned by apparently unrelated third parties.
- Loans are made for, or are paid on behalf of, a third party with no reasonable explanation.
- Loans lack a legitimate business purpose, provide the bank with significant fees for assuming minimal risk, or tend to obscure the movement of fund.

F. Red Flags via International Money Transfer Organizations (Western Union, MoneyGram, RIA etc.)

- Transactions made in multiple, small dollar amounts, indicating that the individual is trying to avoid monitoring systems or transaction reporting rules.
- Customer receives a payment and then sends most or all the amount in separate transactions within a short amount of time (flipping). Flipping is used primarily to avoid law enforcement monitoring.
- Groups of individuals conducting transactions at single or multiple outlet locations or across multiple services.
- The sender knows little or is reluctant to disclose details about the receiver (address or contact information, for example).
- Customer inexplicably travels great distances to an Agent to conduct transactions.
- Customer has no apparent ties to the country where the funds are being sent or collected.
- Customer has been the subject of a law enforcement inquiry known by the Agent.
- Customer offers false identification, whether evident from the identification document or from the document's context with other documents (e.g., use of two or more identification cards that are issued from different countries)
- Customer shows different identification documents or different identification document information (such as phone or address) when coming to your location over time.
- Customer appears to be acting on behalf of a third party, but is not disclosing that information to his Customer Service Officer/ Relationship Manager/Agents, or seems to be nervous or under duress.

Human Trafficking and Human Smuggling

- Customer behaves like they are being controlled by someone.
- Someone else speaks for Customer but puts the transaction in the Customer's name. (This may be done to avoid identifying the true sender or receiver of funds.)

- Customer does not hold their own identification card; someone else holds it for them. This may indicate coercion.
- Customer has bruises, appears malnourished, or has other signs of physical abuse.
- Customer picks up a money transfer and immediately hands the funds to someone else.
- Customer brings in a completed money transfer form in someone else's handwriting.
- Customer does not speak the local language.
- Customer cannot give their name or address without reading from a form.
- Customer seems to lack knowledge of their whereabouts or what city they are in
- Customer appears fearful, anxious, depressed, submissive, tense, nervous, paranoid, or avoids eye contact.
- Multiple smaller dollar amount transactions sent within a short time frame by multiple senders to a common receiver.
- Customer cannot confirm the name of payees they are sending a high value transaction to.
- The customer appears to have no familial or other close relationship with the person to whom they are sending money.
- The customer does not know the name of the person who sent them the money.
- Illegal Gambling.
- The customer indicates to the bank staff that a transaction is for gambling purposes.
- Customer might mention the game (such as Poker, Blackjack, or Bingo), or they may use phrases like: "this is for my losses," "the odds were against me," "playing cards," or "for the horses".
- Customer has an e-mail address containing gambling references.
- Potential Behavioral for Fraud
- The Customer exhibits suspicious behaviour, such as loitering or nervousness, failing to make eye contact, checking phone for directives, scoping out the area.
- Multiple individuals enter a location but only one person transacts. (Often the others will loiter near the door.)
- The receiver admits they have never met the sender or appears coached to state that they have met the sender.
- Potential Fraud Transaction
- Customers who receive multiple transactions under different names or spelling variations
- Customers who receive multiple transactions from different senders in similar or nonstandard dollar amounts in a short amount of time.
- Customers who receive an unusual number of transactions in a short period of time.
- Customers who receive multiple transactions to one receiver with the use of a security question.
- Customers who receive transactions from multiple senders with no apparent family relationship.
- Customers who receive transactions from multiple states, provinces, or countries.
- Customers who frequently both receive and send transactions by one person, especially when transactions are sent to other countries, when the amount received matches the amount being sent, and when Customers who receive transactions immediately attempt to send transactions.

Terrorist Financing "Red flags"

- Persons involved in currency transactions share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self - employed).

- Financial transaction by a non-profit or charitable organization, for which there appears to be no logical economic purpose, or for which there appears to be no link between the stated activity of the organization and other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown, or such activity does not appear to justify the use of a safe deposit box.
- Large number of incoming or outgoing funds transfers takes place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves designated high risk locations.
- The stated occupation of the customer is inconsistent with the type and level of account activity.
- Funds transfer does not include information on the originator, or the person on whose behalf the transaction is conducted, the inclusion of which should ordinarily be expected.
- Multiple personal and business accounts or the accounts of non-profit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries.
- Funds generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from designated high-risk countries.

Other Unusual or Suspicious Activities

- Employee exhibits a lavish lifestyle that cannot be justified by his/her salary.
- Employee fails to comply with approved operating guidelines, particularly in private banking.
- Employee is reluctant to take a vacation.
- Safe deposit boxes or safe custody accounts opened by individuals who do not reside or work in the institution's service area despite the availability of such services at an institution closer to them.
- Customer rents multiple safe deposit boxes to store large amounts of currency, monetary instruments, or high value assets awaiting conversion to currency, for placement in the banking system.
- Customer uses a personal account for business purposes.
- Official Embassy business is conducted through personal accounts.
- Embassy accounts are funded through substantial currency transactions.
- Embassy accounts directly fund personal expenses of foreign nationals.
- The bank shall exercise due diligence in identifying and reporting suspicious transactions.

Section 9.0. Compilation of Reports and Returns to Regulatory Authorities

The Bank shall ensure timely and accurate rendition of all AML/CFT/CPF returns as specified in the CBN AML/CFT/CPF Regulations, 2022, the Money Laundering (Prevention and Prohibition) Act 2022, Terrorist (Prevention and Prohibition) Act 2022, the SEC Rules, and Regulations as well as other relevant Regulations/Acts/Guidelines/Circulars that may he issued from time to time by various government agencies. (See the bank's Regulatory Returns Universe)

Section 10.0. Awareness and Training

The CBN AML/CFT/CPF Regulations, 2022, the Money Laundering (Prevention and Prohibition) Act 2022, Terrorist (Prevention and Prohibition) Act 2022 requires financial institutions to ensure, first, that its employees are made aware of the provisions of the relevant legislation and the

obligations imposed on staff and financial institutions. Secondly, staff shall be given training on how to recognize and deal with transactions which may be related to money laundering or terrorist financing or proliferation financing.

Training in the Bank covers Board members, Executive Management, and all categories of staff. The bank's AML/CFT/CPF training program is a mix of e-learning and instructor-led training modules. The trainings incorporate current developments and changes to the CBN AML/CFT/CPF Regulations, 2022, the Money Laundering (Prevention and Prohibition) Act 2022, Terrorist (Prevention and Prohibition) Act 2022 other related guideline. Changes to internal policies, procedures, processes, and monitoring systems are also covered during the training. There are specialized AML/CFT/CPF training for specialized functions within the Bank. This is to ensure that applicable areas where there are inherent risks within those functions are addressed and how to mitigate the risks are discussed. In addition, on completion of trainings, tests/quiz are given to participants to appraise their level of understanding of the training.

All staff are required to complete the AML/CFT/CPF training at least once every financial year as these forms an integral part of the Bank's employee appraisal. Evidence of completion of the e-learning is kept by the Training Academy. For the instructor led training conducted by the Department/ External facilitators, records are kept by the Training Academy as well as Compliance Department.

The Bank shall also utilize other avenues such as emails to disseminate compliance issues arising from new rules and regulations to all staff.

Section 11.0 Know Your Employee (KYE)/Monitoring of Employee Conduct

Knowing our employees is as important as knowing our customers. An insider can pose the same ML/TF/PF threat as a customer and a criminally co-opted Bank employee might facilitate money laundering, terrorist financing and proliferation financing. The CBN AML/CFT/CPF Regulation 2022 requires:

- That the financial institutions put in place adequate policies, procedures and controls including appropriate compliance management arrangement and adequate screening procedures to ensure high standards when hiring employees, and
- That every Employee's accounts be monitored for potential signs of ML/TF/PF risks and be subjected to the same AML/CFT/CPF Procedures as applicable to other customers' accounts. This is required to be performed under the supervision of the CCO.

11.1 KYE Procedure

The following procedures should be followed and strictly adhered to, to ensure the bank recruits not only the best brains but people equally with good character, high ethical standing, honesty, and integrity.

- KYE information such as background information must be obtained prior to job interview, during job interview and just before offer of employment. Any serious gap observed must be documented and should form part of the basis tor offer of employment.
- All prospective hires must be checked against CBN list of blacklisted individuals prior to offer of employment.
- After acceptance of offer, but before confirmation; background screening cheeks must be conducted to verify the identity of employees,

- Certificates must be verified by awarding institutions. Note to ensure that such credentials are sent to awarding institutions for confirmation along with scanned passport photograph of recipients.
- Employee personal referees must be written and satisfactory report on character and suitability of employment obtained prior to confirmation of employee appointment,
- Former employer must be written, and positive performance and character report obtained prior to confirmation.
- All information supplied by prospective employees must be verified during probation. Any change in such information, including marital status and additional qualifications obtained during the period must be verified against appropriate documents and issuing institutions.

Section 12.0 Anti-Bribery and Corruption Policy

The Bank values its staff highly and has a human resources policy governing its contractual obligations with them as well as benefits they are entitled to.

- Staff are not permitted to accept gifts from customer or suppliers except calendars, diaries, or festive presents of an acceptable nature (that is, where such gifts cannot be construed as bribery, gratification or influencing duty and having substantial commercial value). This shall be in line with the bank's gift policy.
- The use of position/office and taking advantage of the institution to enrich oneself is prohibited.
- Offering gratification to the regulator as an inducement to waive the imposition of penalties arising from failure to comply with laws or regulations is also prohibited.
- Offering/acceptance of gratification to/from customers/potential customers/ suppliers/vendors to do business is prohibited.
- Bribery and corruption are also offences that attract well known consequences such as warning, suspension, termination, or dismissal, depending on the gravity of the offence.

The following is a list of possible scenarios that may arise during an employee or director working for the bank and which may raise concerns under various anti-bribery and anti-corruption laws. The list is not intended to be exhaustive and is for illustrative purposes only to help you in your compliance with this policy.

I. If an employee or director encounters any of these scenarios in the course of his/her work, he/she must report them promptly to the Chief Compliance Officer or use the Whistleblower platform:
II. He/she becomes aware that a third party engages in, or has been accused of engaging in, improper business practices.
III. He/she learns that a third party has a reputation for paying bribes, or requiring that bribes are paid to them, or has a reputation for having a "special relationship" with foreign government officials.
IV. A third party insists on receiving a commission or fee payment before committing to sign up to a contract with us or carrying out a government function or process for the Bank.
V. A third-party requests payment in cash and/or refuses to sign a formal commission or fee agreement, or to provide an invoice or receipt for a payment made.
VI. A third-party request that payment is made to a country or geographic location different from where the third party resides or conducts business.
VII. A third-party request an unexpected additional fee or commission to "facilitate" a service.

VIII. A third party demands entertainment or gifts before commencing or continuing contractual negotiations or provision of services.
IX. A third-party request that a payment is made to "overlook" potential legal violations.
X. An invoice from a third party that appears to be non-standard or customized:
XI. A third-party refuse to put contractual terms agreed in writing:
XII. He/she notices that the Bank e has been invoiced for a commission or fee payment that appears large given the service stated to have been provided.
XIII. H/she is offered an unusually generous gift or offered lavish hospitality by a third party.
XIV. He/she is asked to give hospitality to persons who are not associated with the organization (for example family member)
XV. Or is offered hospitality which extends to persons beyond our business (for example)

Section 13.0 Anti-Slavery Policy

The Bank also adheres to the fundamental human rights enshrined in the Nigerian constitution and does not as a policy permit slavery or encourage the use of employees as slaves.

Section 14.0 Whistle Blowing

The Management of the Bank has a duty to conduct the bank's affairs in a responsible and transparent manner and to consider legal and regulatory requirements. under which the bank operates. The Board of the bank is also committed to the principle of sound corporate governance and behaviour as enunciated of Corporate Governance for banks in Nigeria. One of the several ways a breach of regulatory requirements and staff misconduct can be addressed through a whistle blowing programme.

As such, the whistle-blowing policy and procedures of the Bank are designed to encourage stakeholders to bring unethical conduct and illegal violations to the attention of an internal and or external authority so that action can be taken to resolve the problem.

14.1. Whistleblowing Matters

As a matter of policy, whistleblowing is encouraged within the bank at every stakeholder level. Any of the following matters against the bank or its officers can be brought up for investigation:

- All forms of financial malpractice and impropriety or fraud.
- Improper conduct or unethical behavior.
- Any form of criminal activity.
- Failure to comply with regulatory directive, legal obligations, or statutes.
- Rendition of false returns:
- Falsification of records.
- Forgery (use of false certificates, false declaration of age, etc.
- Actions detrimental to Health and Safety or the environment (SEMS regulations and policies)
- Commission of offense by Premium Trust Bank officers/staff.
- Obstruction of internal/external regulators and auditors.
- Leakage of confidential data.
- Bribery and corruption.
- Abuse of authority.
- Sexual harassment.
- Insider Abuse.
- Non-disclosure of interest.
- Connected transactions.
- Concealment (including attempted concealment) of any malpractice.

- Other forms of corporate governance breaches.

14.2. Whistleblowing Procedure

All stakeholders are provided with whistleblowing channels via the bank's website and in the branches. The whistleblowing channels provide avenue to staff and any other person to report all incidents confidentially and anonymously to various categories of unethical and criminal conduct. This include cases relating to social and environmental risk crystallization associated with projects the bank has financed.

The process of whistleblowing investigation, reporting and general procedure are as contained in the bank's whistleblowing policy.

Section 15.0. Offences and Penalties

15.1. Sanctions Specified in the CBN Anti-Money Laundering/Combating Terrorism Financing/Countering Proliferation Financing Regulations

- The Central Bank of Nigeria prescribes a range of sanctions for failure to comply with the provisions of the AML/CFT/CPF Compliance Regulations. The sanctions provided in the Anti-Money Laundering/Combating Terrorism Financing/Countering Proliferation Financing Regulations are not only proportionate and dissuasive but such that will affect legal persons/financial institutions and their directors/senior management staff also, depending on the requirements breached.
- Any individual, being an official of a financial institution, who fails to take reasonable steps to ensure compliance with the provisions of the Regulations, shall be sanctioned accordingly.
- For purpose of emphasis, the incidence of false declaration or false disclosure by the financial institution or its officers shall be subject to administrative review and sanction as stipulated in AML/CFT/CPF Compliance Regulations.
- Any financial institution, board of directors, senior management or its officer that contravenes the provisions of any of the extant Anti-Money Laundering/Combating Terrorism Financing/Countering Proliferation Financing Regulations shall be subject to applicable sanctions by the CBN in line with the CBN AML/CFT/CPF (Administrative Sanctions) Regulations 2018)

15.2. Sanctions

Non-adherence to the provisions of this Manual shall be treated as an offence. Sanctions shall be applied as stated in the Bank's Disciplinary and Sanctions grid and CBN Administrative Sanctions Regime 2018.

16.0. Conclusion

It is critical to the success of the Bank's Anti-Money Laundering/Combating Terrorism Financing/Countering Proliferation Financing program that all relevant stakeholders comply with the requirements of this policy.

There is the need for all staff to be extra vigilant to ensure that the Bank is not used by criminals to launder the proceeds of their crime, as the repercussions may be unquantifiable.

The policy is not an exhaustive treatise on the subject given the dynamic nature of the regulatory environment and international best practices. This policy shall be read in

conjunction with the CBN AML/CFT/CPF Regulation 2022, the various policies/ manuals of the Bank and other applicable laws.

The AML/CFT/CPF Policy shall be reviewed annually or as frequently as the Board of Directors deems it necessary in the context of regulatory compliance requirements or other business exigencies while any additions prior to the review shall be done as addendums to the policy in the interim.

PremiumTrust Bank

APPENDIX

S/No	Required Action	Infraction	Administrative Sanction/Penalty Deposit Money Bank (DMB)
A. CORPORATE GOVERNANCE AND ROLE OF THE BOARD/MANAGEMENT			
1	AML/CFT/CPF programme that clearly outlines the AML/CFT/CPF policies and procedures of the institution.	* Failure to establish written AML/CFT/CPF policies and procedures.	A minimum penalty as follows: * N20million on the Deposit Money Bank (DMB)
2	Approval of written AML/CFT/CPF policies and procedures	* Failure to approve the AML/CFT/CPF policies and procedures.	A minimum penalty as follows: * N1 million on each member of the board. * N20 million on the DMB.
3	Periodic review and update of the AML/CFT/CPF policies at least every three (3) years	* Failure to review/update the AML/CFT/CPF policies and procedures at least every three (3) years.	A minimum penalty as follows: * N750,000 on the Executive Compliance Officer in the first instance and N750,000 for each year that the contravention continues. * N500,000 on the Chief Compliance Officer in the first instance and N500,000 for each year that the contravention continues. * N5million on the bank in the first instance and N1,000,000 for each year that the contravention continues.
4	Communication of the AML/CFT/CPF program across the institution and ensuring that it is effectively implemented.	* Failure to communicate the AML/CFT/CPF program of the organization to employees.	A minimum penalty as follows: * N750,000 on the Executive Compliance Officer. * N500,000 on the Chief Compliance Officer. * NI0million on the DMB.
5	Supervision of implementation of the AML/CFT/CPF program, risk management and reporting requirements by the Board.	* Failure of the Board or its Committee to supervise and ensure the effective implementation of the AML/CFT/CPF program.	A minimum penalty as follows: * N500,000 on each member of the Board. * N10million on the DMB.

6	Receive, review, and provide feedback on periodic reports on AML/CFT/CPF issues submitted by senior management.	* Failure of the Board to review and provide feedback to Management on reports that it receives on AML/CFT/CPF issues.	A minimum penalty as follows: * N500,000 on each member of the Board. * N5million on the DMB.
7	Generate periodic reports on AML/CFT/CPF issues to the Board or its relevant Committee(s).	* Failure of the Officer to generate periodic reports on AML/CFT/CPF issues to the Board or its relevant Committee.	A minimum penalty as follows: * N750,000 on the Executive Compliance Officers. * N-500,000 on the Chief Compliance Officer. * N5million on the DMB.
8	Formulation and issuance of Code of Conduct/Ethics to staff that includes observance of ethical requirements relating to AML/CFT/CPF.	* Failure to formulate, issue and ensure the observance of a Code of conduct/ethics that includes AML/CFT/CPF by staff.	A minimum penalty of N5million on the DMB.
9	Put in place management information systems to monitor, detect, analyze, and generate reports on suspicious transactions.	* Failure to put in place an information system to monitor, detect, analyze, and generate reports on suspicious transactions.	A minimum penalty of N5million on the DMB.
B. RISK MANAGEMENT:			
S/No	**Required Action**	**Infraction**	**Administrative Sanction/Penalty Deposit Money Bank (DMB)**
10	Embedding of ML/TF/PF Risks in overall Risk Management Framework of the financial institution.	* Failure to recognize ML/TF risk in the Risk Management Framework.	A minimum penalty of N5 million on the DMB in the first instance and N1million for each year that the contravention continues.
11	Put in place ML/TF/PF risk classification system.	* Failure to classify ML/TF risk in the bank. * Failure to put in place guidelines for risk assessment and profiling of customers in the institutions AML/CFT/CPF board approved program. * Failure to carry out risk assessment and profiling of each account.	*A minimum of N1million on the Chief Risk Officer of the DMB. *A minimum penalty of N3million on the DMB for failure to put in place guidelines for risk assessment and profiling of customers in the AML/CFT/CPF program. * A minimum of N100,000 per account for failure to carry out risk assessment and profiling of the account.

12	Put in place a policy for the prohibition of numbered accounts, anonymous accounts, or accounts in fictitious names and shell companies.	Non-existence of policy on prohibition of numbered or anonymous accounts, or accounts in fictitious names, and shell companies, from doing business with the bank.	A minimum penalty as follows: * N1million on each member of the Board * N15million on the DMB.
13	Establishment of a screening mechanism for PEPs, UN sanctioned persons/entities list, other official lists, and internally generated lists of high-risk customers	* Failure to establish screening mechanism for PEPs, UN sanctioned persons/entities lists, and internally generated lists of high-risk customers.	A minimum penalty of N15 million on the DMB.
14	Consideration of ML/TF/PF risks in approving expansion of business e.g., new branches, and markets (domestics and foreign), new products/services.	* Failure of the Board and management to consider and document ML/FT/PF risks as part of the approval process for the expansion of business (including introduction of new products and services).	A minimum penalty of N2million on the DMB.
C. POLICIES AND PROCEDURES ON CUSTOMER DUE DILIGENCE (CDD):			
S/No	**Required Action**	**Infraction**	**Administrative Sanction/Penalty Deposit Money Bank (DMB)**
15	Establishment of written and Board-approved policies and procedures on CDD/KYC requirements.	* Failure to establish written policies and procedures on CDD/KYC requirements.	A minimum monetary penalty as follows: * N1million on each member of the Board. * N15million on the DMB. * Where the contravention persists after three consecutive penalties, the Board may be suspended or removed.
16	Implementation of AML/CFT/CPF policies and procedures in all branches including, foreign branches and subsidiaries, if applicable.	*Failure to implement AML/CFT/CPF policies and procedures in all branches (including foreign branches and subsidiary).	* A minimum of N1,250,000 on the Executive Compliance Officer. * A minimum penalty of N1,000,000 on the Chief Compliance Officer. * A minimum penalty of N20million on the DMB.
17	Implementation of CDD measures for Customer Identification **(whether permanent or occasional, natural, or**	* Failure to implement CDD measures for **Customer Identification.**	* A minimum ofN750,000 on the Executive Compliance Officer. * A minimum penalty of N500,000 on the Chief Compliance Officer.

	legal persons, or legal arrangements, etc.)		* A minimum penalty of N1million per customer.
18	Implementation of CDD measures for verification of customer identification using reliable, independent source documents, data, or information	* Failure to implement CDD measures for **verification of Customer Identification.**	* A minimum of N750,000 on the Executive Compliance Officer. *A minimum penalty ofN500,000 on the Chief Compliance Officer. *A minimum penalty of N1million per customer.
19	Obtain information on the beneficial owner of accounts, where a customer is an intermediary or authorized representative of another party, including but not limited to the following information listed in Regulation 15 of CBN AML/CFT/CPF Regulations, 2013: (a) Legal relationship and authority, such as evidence of attorney, resolution, and similar mandates. (b) Information on the source of funds/wealth of the ultimate beneficial owner. (c) Identity of management and principal owners/controllers of a company being represented. (d) Similar information on the procedure for acceptance of individual customers.	* Failure to obtain information on the beneficial owner where a customer is an intermediary or authorized representative of another party.	*A minimum penalty of N1,250,000 on the Executive Compliance Officer. *A minimum penalty of N1million on the Chief Compliance Officer; *A minimum penalty of N1million per customer.

20	Classification of customers into designated risk categories and apply customer due diligence (CDD) accordingly.	* Failure to classify customers into designated risk categories and apply CDD accordingly.	*A minimum penalty ofN750,000 on the Executive Compliance Officer. * A minimum penalty ofN500,000 on the Chief Compliance Officer; * A minimum penalty of N7million on the DMB

D. POLICIES AND PROCEDURES ON MAINTENANCE OF RECORDS:

S/No	Required Action	Infraction	Administrative Sanction/Penalty Deposit Money Bank (DMB)
21	Maintenance of CDD and transaction records (in electronic/paper form, onsite/offsite storage) for at least 5 years	* Failure to maintain records obtained through CDD measures and transaction records for at least 5 years after cessation of relationship in hard and soft copies.	A minimum penalty of N10 million on the DMB.
22	Establish a record keeping system that is easy to retrieve on a timely basis.	* Failure to establish a record-keeping system that facilitates easy retrieval of records on a timely basis	A minimum penalty of N5 million on the DMB.

E. MONITORING OF SUSPICIOUS TRANSACTION REPORTING

S/No	Required Action	Infraction	Administrative Sanction/Penalty Deposit Money Bank (DMB)
23	Maintenance of an internal system (automated/manual) for detecting and reporting unusual and suspicious activities.	* Failure to maintain an internal system for detecting and reporting unusual and suspicious activities.	A minimum penalty of N10million on the DMB.
24	Rendition of suspicious transaction reports to relevant authorities.	* Failure to render reports on suspicious transactions to the NFIU.	* A minimum penalty is as follows: * N2,500,000 on the Executive Compliance Officer: * N2.000,000 on the Chief Compliance Officer. * N20million on the DMB.
25	Rendition of other AML/CFT/CPF Reports (such as Crossfires) to relevant authorities, such as NFIU and CBN.	* Failure to render AML/CFT/CPF Reports (other than STR) to the relevant authorities.	* A minimum penalty as follows: * N1,250,000 on the Executive Compliance Officer. * N1,000,000 on the Chief Compliance Officer. * N15million on the DMB.

26	Timely rendition of AML/CFT/CPF reports to the relevant authorities.	* Late rendition of AML/CFT/CPF Reports/Returns to the relevant authorities	A minimum penalty as follows: * N750,000 on the Executive Compliance officer. * N500,000 on the Chief Compliance Officer. * N5million on the DMB in the first instance. * N200,000 for each day that the contravention continues.
27	Maintenance of monitoring systems for terrorism finance.	Failure to maintain specific monitoring systems for terrorism finance.	A minimum penalty as follows: * N1,250,000 on the Executive Compliance Officer. * N1,000,000 on the Chief Compliance Officer. * N10 million on the DMB.
28	Analysis of reports from the operational units by the AML Compliance unit/department and generate appropriate Management Report.	* Failure of the AML Compliance officer/unit to analyze reports from the operational units for management consideration.	A minimum penalty as follows: * N750,000 on the Executive Compliance Officer. * N500,000 on the Chief Compliance Officer. * N800,000 on the MD/CEO.
29	Put in place and observe confidentiality procedures and security measures to prevent the disclosure of information on unusual and suspicious transactions to unauthorized parties, intentionally or unintentionally.	* Failure to put in place and observe confidentiality procedures and security measures to prevent disclosure of information on unusual and suspicious transactions to unauthorized parties.	A minimum penalty as follows: * N500,000 on any officer that breaches the confidentiality procedures and security measures put in place by the DMB. * N2million on the DMB for failure to put in place appropriate measures and procedures.
30	Put in place a mechanism to monitor politically Exposed Persons (PEPs).	* Failure to put in place specific monitoring mechanisms for PEPs.	A minimum penalty of N2million on the DMB.
31	Put in place policy to protect employees when they report suspicious transactions, in good faith.	* Failure to put in place policy to protect employees when they report suspicious transactions in good faith.	A minimum penalty of N2million on the DMB.

32	Imposition of sanctions on employees that do not adhere to the monitoring and reporting policies and procedures of the financial institution	* Failure to sanction employees that do not adhere to the monitoring and reporting policies and procedures	A minimum penalty of N2million on the DMB.
F. INTERNAL AUDIT/CONTROL AND EXTERNAL AUDIT			
S/No	**Required Action**	**Infraction**	**Administrative Sanction/Penalty Deposit Money Bank (DMB)**
33	The internal Audit department/unit should have the competency to conduct oversight on the AML/CFT/CPF compliance function of the financial institution.	* Failure of the Internal Audit department/unit to competently oversee the compliance function of the financial institution	A minimum penalty of N5million on the DMB.
34	Periodically review and test compliance with the AML/CFT/CPF program, CDD/KYC policies and procedures and follow-up on findings.	* Failure of the internal audit unit to review and test compliance with the AML/CFT/CPF program, CDD/KYC policies and procedures and follow up on findings.	A minimum penalty as follows: *N1million on the Internal Auditor. * N5million on the DMB.
35	Review the AML/CFT/CPF Program document within event 3 years from the last review.	* Failure to review the AML/CFT/CPF program periodically as prescribed	A minimum penalty as follows: * N1,250,000 on the Executive Compliance Officer * N1million on the Chief Compliance Officer. * N5million on the DMB.
36	Review of the audit reports on AML/CFT/CPF by the Board	* Failure of the Board to review the AML/CFT/CPF audit report.	A minimum penalty as follows: * N500,000 on each member of the Board. * N5million on the DMB.
37	Risk-based internal audit and specific review of compliance with policies and procedures for PEPs and other high-risk clients and activities	* Failure to conduct specific review of compliance with policies and procedures for PEPs and other high-risk clients.	A minimum penalty as follows: * N500,000 on the Internal Auditor. * N1miliion on the DMB
38	Ensure that the internal audit staff possess the requisite professional/academic qualification, experience, and competence.	* Failures to put in place qualified, experienced, and competent internal audit staff as stipulated in the Approved Persons Regime.	A directive to the DMB to take immediate steps to appoint a suitably qualified internal auditor within a reasonable time frame to be determined by the CBN. Failure of the DMB to

			comply with the CBN directive shall attract a minimum penalty as follows: * N5million one-off fine on the DMB at the expiration of the CBN deadline. *N100,000 on the DMB for each day the contravention continues.
G. COMPLIANCE FUNCTION			
S/No	**Required Action**	**Infraction**	**Administrative Sanction/Penalty Deposit Money Bank (DMB)**
39	Appointment of a chief compliance officer of appropriate status within the organization with clearly defined roles and responsibility	* Failure to appoint an AML/CFT/CPF compliance officer of appropriate status with clearly defined roles and responsibilities	A minimum penalty as follows: * N500,000 on each member of the Board. * N10million on the DMB.
40	Adequacy of resource allocation to the compliance function such as budgetary allocation and number of staff skilled in AML/CFT/CPF.	* Failure to allocate adequate resources to the AML/CFT/CPF compliance function	* N1 million penalty on each Board member. * N2million on the DMB.
41	Appointment of an AML/CFT/CPF compliance officer in each office/ branch/subsidiary or cluster thereon (as approved by the CBN).	* Failure to appoint an AML/CFT/CPF compliance officer in each office/ branch/subsidiary or branch/subsidiary or cluster area.	A minimum penalty as follows: * N500,000 on each member of the Board * N10million on the DMB.
42	Establishment of Group compliance function that has clearly defined relationship with the subsidiary(ies)	* Absence of group compliance function with clearly spelt out relationship with the subsidiaries	A minimum penalty as follows: * N500,000 on each member of the Board * N10million on the DMB.
H. TRAINING			
S/No	**Required Action**	**Infraction**	**Administrative Sanction/Penalty Deposit Money Bank (DMB)**
43	Implement an approved annual AML/CFT/CPF Training Plan for all categories of employees	* Failure to implement an approved annual an approve annual for employees	A minimum penalty as follows: * N750,000 on the Executive Compliance Officer. * N500,000 on the Chief Compliance Officer. * N5million on the DMB.

44	Render quarterly returns on level of compliance with approved annual AML/CFT/CPF Training programme (containing categories, frequency, and types of trainings) for employees to the CBN and NFIU.	* Failure to render quarterly returns on training to the CBN and NFIU	A minimum penalty as follows: * N750,000 on the Executive Compliance Officer * N500,000 on the Chief Compliance Officer for failure to prepare the AML/CFT/CPF training budget. * N5million on the DMB for failure to approve and conduct AML training and render returns to the CBN.
45	Board and Management participation in AML/CFT/CPF Training	* Failure of Board and Management to participate in AML/ CFT training.	A directive to the DMB to take immediate steps to sponsor or organize the training within a reasonable time frame to be determined by the CBN. Failure of the DMB to comply with the CBN directive shall attract a minimum penalty as follows: * N5million one-off fine on the DMB at the expiration of the CBN deadline. * N1million on the DMB for each day the contravention continues.
46	Organize or sponsor professional AML/CFT/CPF trainings for Chief Compliance Officer/ Compliance Officer.	* Failure to expose Chief Compliance Officers to professional training/courses on AML/CFT/CPF.	A directive to the DMB to take immediate steps to sponsor or organize the training within a reasonable time frame to be determined by the CBN. Failure of the DMB to comply with the CBN directive shall attract a minimum penalty as follows: * N5million one-off fine on the DMB at the expiration of the CBN deadline * N100,000 on the DMB for each day the contravention continue

47	Ensure attendance of AML/CFT/CPF trainings by all staff	* Failure to put in place mechanism for ensuring attendance at AML/CFT/CPF trainings for all staff.	A minimum penalty of N5million on the DMB.
48	Communicating new AML/CFT/CPF laws/policies to employees.	* Failure to communicate or educate employees on new AML/CFT/CPF laws/policies.	A minimum penalty as follows: * N750,000 on the Executive Compliance Officer. * N500,000 on the Chief Compliance Officer. * N5million on the DMB.