Unity Bank Plc
Anti-Money Laundering
&
Combating the Financing of Terrorism & Combating Proliferation Financing
Control Policy Manual

Edition:	**2022**
Approved by:	Board of Directors
Recommended by:	Executive Committee (EXCO)
Next Review:	Annual
Contact Person:	Abubakar Siddiki Adamu Ag, Chief Compliance Officer (CCO) Compliance Group Unity Bank Plc Email: regulatorycompliance@unitybankng.com Mobile: +234-8070691264

TABLE OF CONTENTS **PAGE**

1.0 INTRODUCTION

The purpose of this manual is to summarize detail of Anti Money Laundering, Combating the Financing of Terrorism and Combating Proliferation Financing (AML/CFT/CPF) obligations on the Directors and Employees of Unity Bank Plc (the Bank) in relation to their conduct and to chart the information which the Bank is required to impart to all Directors and employees in respect of the regulations which affect the banking and investment business carried on by the Bank.

The explanation of rules contained in this manual is not exhaustive and in case of need/ advice the Compliance Group may be contacted. This Manual applies to all bank staff. Every employee must have access to this Manual. Each section of the Manual contains a summary of the relevant rules, as well as the relevant operating procedures, for each functional area of the business.

Banking is authorized and regulated in Nigeria by the Central Bank of Nigeria (CBN). The current legal framework within which the CBN operates is the CBN Act of 2007 which repealed the CBN Act of 1991 and all its amendments. This manual is aimed at making Directors and staff aware of their regulatory obligations. This manual outlines the procedures which have been put in place to ensure compliance with the CBN and other Regulators requirements.

This Manual is not a static document; it will continue to be reviewed annually or as the need arises to reflect changes in both the laws and regulations in line with CBN requirement. The regulations embody good business practice and reflect the high AML/CFT/CPF principles.

2.0 POLICY STATEMENT:

Unity Bank Plc is committed to comply with the AML/CFT/CPF Laws and Regulations of all competent Authorities and Jurisdictions.

In addition to adopting best practices; ethical and legal considerations shall always guide our commercial decisions. Our Directors, Staff and other relevant Stakeholders shall fully understand and be guided by the AML/CFT/CPF standards.

Protecting the good name and the reputation of the Bank shall be the primary consideration in all actions taken by the Board and Management. In this regards the Bank has acquired the necessary software to enable it monitor all compliance issues by various Branches and Business Groups and also to identify Suspicious Transactions based on specified parameters for further Investigation and Reporting.

The Bank shall continue to protect its products and services from being used for the purpose of Money Laundering, Terrorism Financing and other crimes through investment in Training, adequate Staffing and the use of appropriate Technology.

We aim to maintain the highest operating standards to advance the interest of our Stakeholders. We shall cooperate fully with all Regulators and Law Enforcement Agencies in all AML/CFT/CPF activities.

In our resolve to ensure improved AML/CFT/CPF activities and strengthen our Policy and Procedures, we subject our compliance to examination by our Internal Audit, Internal Control, External Auditors and all Regulatory Bodies.

Additionally, we also have in place a Know Your Customer (KYC) Handbook. This is all in an effort to ensure full compliance with all AML/CFT/CPF Laws and Regulations that may be so issued and or enacted from time to time. In this regard the following reflects the minimum AML/CFT/CPF Controls requirement as detailed in the policy:

i. Appointment of designated officers i.e. Executive Compliance Office (ECO), Chief Compliance
ii. Officer (CCO) and Money Laundering Reporting Officer (MLRO).
iii. Customer Due Diligence (This includes requirements for “Know Your Customer” (KYC) principles, sanctions screening and Enhanced Due Diligence measures – for customers, vendors and partners; representing higher ML/TF/PF risks;
iv. Suspicious transactions and activities monitoring and reporting, internally and to relevant Financial Intelligence Authority;
v. Continuous Training and awareness for Board members and employees on the fulfilment of their AML/CFT/CPF obligations;
vi. Record keeping and retention for prescribed periods; and
vii. Monitoring of AML/CFT/CPF compliance by way of periodic reviews conducted by Internal Audit and assigned independent assurance functions.

Tomi Somefun
Managing Director / Chief Executive Officer
Unity Bank Plc

3.0 POLICY OBJECTIVES:
This Policy clearly sets out our approach to the identification, mitigation and management of the AML/CFT/CPF risks that we can reasonably anticipate. We have been guided by relevant local laws and regulations and internationally established banking practices and standards to ensure that:

- To ensure adequate support to business areas to effectively manage regulatory and statutory risks in business operations
- The AML/CFT/CPF Compliance policy is adequate and meet the banking practices and standards.
- We administer and maintain an effective program for compliance with the Regulations.

The thrust of this manual is to describe in clear terms the policy, procedures and controls to be applied in the handling of AML/CFT/CPF issues in the establishment of account relationships and processing of products / transactions. The objective is to provide a uniform understanding of the requirements for handling of various transactions that could subject The Bank to AML/CFT/CPF risks.

The purpose of the Policy therefore, is to establish the essential standards designed to prevent the Bank from being used for money laundering and terrorism financing. This is in line with the global resolve to prevent and fight money laundering and terrorist activities, by establishing governing standards to guide banking relationships and transaction processing.

It is expected that this policy will be used in all Unity Bank locations. The Bank shall examine its anti-money laundering strategies, goals and objectives on an ongoing basis and maintain an effective AML/CFT Policy for the Bank's business. Specifically, the Policy objectives include:

- To provide a guide aimed at preventing Money Laundering and Terrorist financing activities within the Bank

- To provide our products and services only to customers whose identities and nature of business transactions have been reasonably ascertained

- To avoid relationships with those that we reasonably assess as posing unacceptable risks of money laundering or terrorism financing and assess the viability of maintaining ongoing relationships with customers that fit these criteria

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

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

- Manage changes to our products, business processes and systems to ensure that money laundering and terrorist financing risks are identified and managed.

4.0 POLICY SCOPE:

This Policy document focuses specifically on Anti-Money Laundering/Combating Financing of Terrorism issues. It sets out at a high level, the key AML/CFT/CPF Policies that the Bank operates in relation to all of its business areas or concerns.

The Bank shall ensure the basic tenets of Anti Money Laundering I.e. Know Your Customer (KYC)/ Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Source of funds and destination of funds have been covered in this Policy document.

It also covers the Regulatory and Institutional framework, Risk rating of products and customers, Processes, Controls, Customer Due Diligence, Procedures for monitoring, evaluation of implementation, response to compliance failures and other AML/CFT/CPF requirements.

The Policy reflects the minimum requirements in respect of Anti-Money Laundering and Combating the Financing of Terrorism Controls and may be supplemented by Internal Policies and Procedure Manuals where the Internal Policies and Procedure are more stringent.

4.1 POLICY OWNERSHIP:

The responsibilities connected with this Policy are:

- The overall ownership of this document rests with the Executive Compliance Officer (ECO) of the Bank.
- The day to day custodian of the Policy document is the Compliance Group.
- No changes or exceptions from this Policy are allowed without the formal agreement of the Chief Compliance Officer and the Executive Compliance Officer (ECO) and subsequent approval of the Bank's Board of Directors.

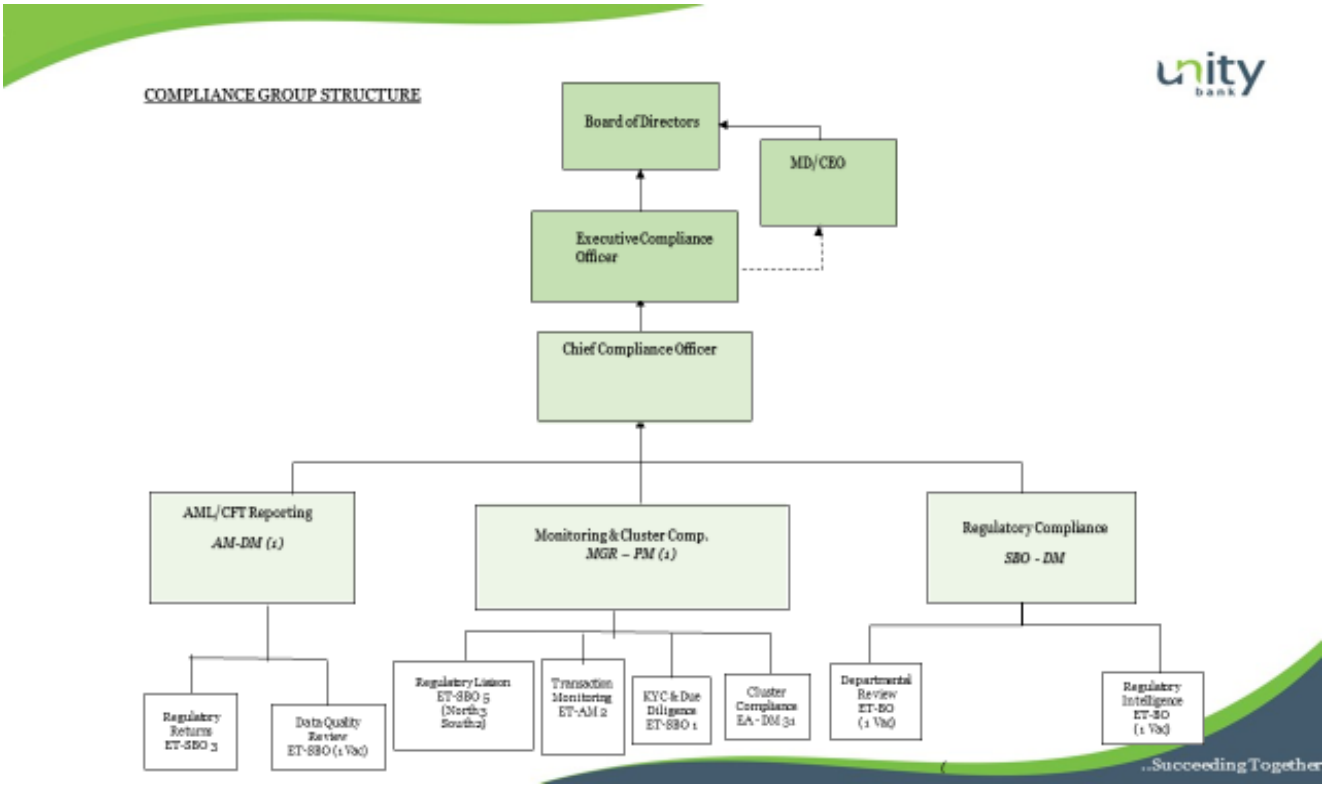
4.2 POLICY FOCUS:

The Policy adopts the Risk Based Approach (RBA) to specify the minimum standards in handling the various aspects of AML/CFT/CPF Compliance with regards to:

- ✓ Know Your Customer (KYC)
- ✓ Simplified Due Diligence
- ✓ Enhanced Due Diligence
- ✓ Cross Border Correspondent Banking
- ✓ Sanction Screening
- ✓ New Technologies and Non-Face to Face Transactions
- ✓ Wire Transfers
- ✓ Customer Risk Profiling
- ✓ Reporting
- ✓ Monitoring of Transactions

- ✓ Record Preservation
- ✓ AML/CFT/CPF Compliance Training
- ✓ Trade Based ML/FT/PF

4.2.1 Compliance Group Structure



4.3 ROLES AND RESPONSIBILITIES:

4.3.1 Board of Directors:

a. The Board of Directors has the responsibility for approving the AML/CFT/CPF policy

b. Understanding the major risks confronting the Bank, and setting acceptable levels for these risks.

c. The Board shall also ensure that Senior Management takes steps necessary to identify, measure, monitor, and control these risks.

d. The Board shall provide governance guidance and oversight to Senior Management.

e. Overseeing the Management of the AML/CFT/CPF Risks by Senior Management.

f. Appointment of the Chief Compliance Officer (CCO).

g. At least annually, through Internal Audit Group or AML/CFT Consultants, assess the extent to which the Bank is managing its AML/CFT/CPF Compliance.

h. Receives and reviews AML/CFT/CPF Compliance report from the CCO. However, may delegate this to a Board Committee.

4.3.2 Executive Management

a. Approves and minutes any exceptions or deviations allowed in terms of this Policy

b. Adopts the AML/CFT/CPF Policy and Procedure Manual before Approval by the Board

c. Ensures appropriate AML/CFT/CPF Policies, Procedures and Processes ("systems and controls") have been set up

d. Ensures Staff receive appropriate and timely AML/CFT/CPF Compliance Training.

e. Ensures AML compliance function is adequately resourced with personnel and funding.

f. Ensures appropriate AML/CFT/CPF compliance culture exists within the Bank

g. Ensures non-compliance is appropriately sanctioned

4.3.3 Executive Compliance Officer

a. The Executive Compliance Officer is responsible for ensuring the rules and principles set by the CBN and other Regulators are being adhered to with the needed support of the Chief Compliance Officer, Bank's Staff, Management and Board.

b. Responsible and accountable for any breach of any extant regulation in the bank.

c. Ensures rendition of all returns both in soft and hard copies to the CBN or as may be required by other regulatory or law enforcement body.

d. Advises the Executive Committee (EXCO), Senior Management and Bank personnel of emerging Statutory and Regulatory **COMPLIANCE ISSUES** and consults and guides the Bank in the establishment of controls to mitigate risks.

e. Promotes Compliance Culture in the Bank.

f. Relationship Management with Regulatory Bodies.

g. Presents Compliance Report to the Board.

h. Participates in various committees, audits and examinations.

4.3.4 Chief Compliance Officer

a. Support the ECO in ensuring that the rules and principles set by the CBN and other Regulators are being adhered to with the needed support of the Bank's Staff, Management and Board.

b. The Chief Compliance Officer is responsible for developing, implementing and administering all aspects of the Bank's Statutory and Regulatory Compliance Program.

c. Participates in various committees, audits and examinations.

d. Ensures Training of Bank Staff on Anti-Money Laundering and Combating Financing of Terrorism.

e. Promotes Compliance Culture in the Bank.

f. Ensuring full compliance with all Anti-Money Laundering Reporting requirements of the Regulatory Agencies.

g. Reviews and approves Suspicious Transactions Report (STR)/High Risk Customers' transactions with a view to escalating STR to NFIU.

h. Developing policies and programs that encourage Managers and Employees to report suspicious transaction(s) without fear of retaliation.

i. Developing, coordinating and participating in multifaceted educational and training programs that focus on the elements of the compliance programme and seek to ensure that all appropriate employees and Management Staff are knowledgeable of and comply with all compliance programmes.

j. Developing materials at an Institutional level for distribution/hoisting on the Bank's portal for all employees to enhance awareness of compliance activities including posters when need be.

k. Annual review of the Bank AML/CFT/CPF Policy Manual in line with the CBN requirement.

l. Coordination of the Bank's Examination/Spot Checks by Regulatory Bodies.

m. Coordination and ensuring prompt rendition of all statutory returns by all the Departments in the Bank.

n. Relationship Management with Regulatory Bodies.

4.3.5 Compliance Group:

Compliance Group is responsible for assisting the Executive Management and Board in effectively managing the compliance risk faced by the Bank by:

i. Developing, reviewing and maintaining AML/CFT/CPF Policy

ii. Monitoring adherence to AML/CFT/CPF Policy;

iii. Raising awareness in terms of AML/CFT/CPF Policy

iv. Advising Employees, Line Managers and Business Units of AML/CFT/CPF Policy

v. Conducting regular AML/CFT/CPF Compliance Training or Programmes in line with the requirements or provisions of the Money Laundering Prohibition Act 2011 (as amended)

vi. Ensure there is adequate compliance infrastructure

vii. Ensures relevant statutory reports or returns are rendered to regulatory authorities.

viii. Ensure effective Communication of circulars and guidelines to Executive Management and relevant Department of the Bank.

ix. Ensure proper record keeping of all circulars and guidelines issued by the Regulatory Authorities

x. Ensuring prompt rendition of all Regulatory and Statutory Returns to appropriate Regulatory Authorities

xi. Place special surveillance on High Risk Customer's account transactions

xii. Ensure that proper and appropriate Customer Due Diligence procedures is conducted in line with standard practices during Account opening and when necessary

xiii. Develop and ensure proper KYC Procedures are enforced in the Bank.

xiv. Maintain watch-lists of high risk accounts.

xv. Ensure strict adherence of the Bank to the CBN guidelines, regulations and other laws.

4.3.6 Compliance Officer

a. Ensure full compliance with all Anti-Money Laundering, Combating the Financing of Terrorism and Combating Proliferation Financing Laws and Regulations. Prompt Reporting of all Regulatory and Statutory Requirements from Regulatory Bodies and Agencies.

b. On a daily basis, review all existing and newly opened accounts and ensure complete Account Opening Documentation (KYC) is in place. Follow-up on accounts with incomplete documents and / or deferrals for full compliance.

c. Ensures review of high risk customers account transactions to determine money laundering and terrorist financing transactions. In case of detection of a suspicious transaction,escalate suspicious activities to regulatorycompliance@unitybankng.com. Also forward the Suspicious Transactions Report (STR) immediately and without delay to the Chief Compliance Officer for his/her review, approval and filling to the NFIU.

d. Ensure branches comply with Know Your Customer (KYC)/ Know Your Customer Business (KYCB) and conduct Enhanced Due Diligence (EDD) processes /Procedures on all High Risk Customers.

e. Compilation of Branch Politically Exposed Persons (PEPs) List and rendition of Monthly report of same to Compliance Group.

f. Ensures Enhanced Due Diligence is conducted at onboarding of PEP accounts or other high risk accounts and same are duly approved by Zonal Head/ Executive Director in case of PEPs and Regional Manager in case of other high risk accounts. The approval form must be filed in the respective mandate files.

g. Ensuring the use of the Blacklisted Individuals and Organizations Portal to screen existing and prospective Customers on the Terrorist Targeted list (negative lists) to avoid opening of account for Terrorist and Terrorist Organizations. Matching names of Individual and Organizations should be promptly reported to Compliance Group.

h. Ensure all Designated Non-Financial Businesses and Professions Institutions (DNFBPs) Customers register and obtain Certificate of Registration from Special Control Unit against Money Laundering (SCUML), and copy of the Certificate duly filed in relative Customer's Mandate file.

i. Review all existing and newly opened accounts to ensure Customer Account Information are properly captured on the Banking Application. Ensure missing information is updated by the branch.

j. Conduct regular AML/CFT/CPF Training for all Staff to ensure the needed sensitization on AML/CFT?CPF Laws and Regulations.

k. Review all Regulatory Websites (CBN, NDIC, SEC, NSE etc.) to ensure compliance with Regulatory Circulars.

4.3.7 **Employee**:

All employees of the Bank must:

i. Familiarize themselves with the content of the Policy
ii. Familiarize themselves with all applicable laws and regulations
iii. Take responsibility for compliance with this policy as it applies to them in accordance with their roles and responsibilities and;
iv. Take responsibilities for their compliance with laws, rules and standards and their adherence to the Bank's procedures, systems and controls.
v. Ensure proper and complete Customer Due Diligence procedures are carried out where necessary especially during Account Opening for Customers
vi. Exhibit tact in identifying and reporting suspicious transactions / activities using the appropriate reporting line. Avoid customer tip-off
vii. Adhere strictly to record retention or preservation policy of the Bank, especially as it relates to the provision of Section 7 of the Money Laundering Prohibition Act 2011 (as amended)
viii. Attend and demonstrate competence from the knowledge and skills imbibed from AML/CFT/CPF Compliance training.

5.0 STATUTORY OBLIGATIONS UNDER WHICH EMPLOYEE MAY BE HELD LIABLE FOR NON COMPLIANCE AND BREACHES OF AML/CFT/CPF REGULATIONS

Unity Bank employee who suspects Money Laundering activities has a responsibility to report such suspicions (concerning customer, transaction or account) to the Compliance Officer at the branch or the **Chief Compliance Officer**, at the Head Office. While reporting suspicion(s), Staff are not expected to intimate or warn the customer involved of the action taken. This will amount to "**Tipping Off**" which is a criminal offence under Nigeria's Anti-Money Laundering laws and Terrorism Acts (Terrorism Act 2011 as amended, Money Laundering Act 2011 as amended, Central Bank of Nigeria Anti- Money Laundering

and Combating the Financing of Terrorism in Banks & Other Financial Institutions in Nigeria Regulations, 2013, as amended and CBN/AML CFT Administrative Sanction, 2018 etc.). Employee who fails to comply shall be liable to civil and or criminal penalties including but not limited to administrative penalties, fines and damages. Failure to adhere to this policy may subject Unity Bank employees to disciplinary action and up to and including the termination of employment. Violation of AML/CFT laws may also subject employees to imprisonment while the Bank faces reputational, operational, legal and financial losses.
Similarly, non-Compliance with the Bank's AML/CFT Policy controls that constitutes material breaches shall attract stiff sanctions as follows:

(a) Payment of fines of up to ₦ 1 million
(b) Imprisonment of between 2 years and 5 years
(c) Confiscation of assets linked to the offence
(d) Suspension from practicing the profession for 5 years
(e) All of the above

However, where a staff carries out his/her duty in good faith, such an individual shall not be liable to any civil/criminal liability or criminal/civil proceedings. The law also protects both the Bank and members of staff from being sued by customers for breach of confidentiality if they report a suspicion of money laundering.

The MLPA also creates additional offences that are particularly relevant for Financial Institutions and their employees as detailed below:

Offence	**Details**	**Recommended Punishment**
Collaboration /providing assistance	Providing assistance to a Criminal and/or Terrorist to obtain, retain or invest proceeds of crime, Terrorist Asset or, who should have known or suspected the funds were of criminal/terrorist financing origin. It is however a defense that the person concerned reported their knowledge or suspicion to the law enforcement agencies at the first available opportunity and discontinue the action connoting the assistance	Imprisonment for a term not less than 5 years but not more than 10 years
Tipping off	Giving information to a suspect of crime or terrorism that they are subject of a suspicious transaction report or that a disclosure has been made or that the law enforcement authorities are carrying out an investigation	Maximum of 3 years imprisonment and/or a fine
Failure to report	Failure to make a suspicious transaction report as soon as is reasonably practical after the information came to their attention to the delegated person (usually the CCO or his representative in the branch) after knowledge,	A maximum of 3 years' imprisonment or fine or both

	suspicion or reasonable grounds for suspicion of money laundering and suspected terrorist funding. The duty to report also covers situations when the business or transaction has been turned away or has not been proceeded with because the circumstances were considered suspicious.	
Non-Compliance	Non-implementation of effective policies and procedures	Revocation of license, imprisonment or fine

All Staff are therefore expected to read and fully understand this Manual to aid them on their schedule. Every employee of the Bank is expected to sign the attached Form (appendix) confirming his/her understanding of obligations and duties as contained in this policy.

6.0 TREATMENT OF UNUSUAL AND SUSPICIOUS TRANSACTIONS

It is mandatory for all Staff of Unity Bank to observe confidentiality in all aspect relating to suspicious transactions/activities as it is an offence to disclose information on unusual and suspicious transactions/activities to unauthorized parties. All Officers involved in processing unusual and suspicious transactions/activities are expected to ensure safety measures are employed to prevent disclosure of information on such transactions.

6.1 REWARDS FOR INDIVIDUAL AND COLLECTIVE EFFORTS IN DETECTING MONEY LAUNDERING AND FINANCING OF TERRORISM

The Management of the Bank will frequently appreciate individual and collective efforts of Staff towards the prevention and detection of Money Laundering and Financing of Terrorism through the system by way of formal commendation and other forms of incentives.

6.2 PROTECTION OF EMPLOYEES WHO REPORT SUSPICIOUS TRANSACTIONS

Employees who report suspicious transactions in good faith will not be victimized in any way.

6.3 MONITORING OF EMPLOYEES' CONDUCT

In line with Section 38 of the CBN AML/CFT Regulations 2013, employee accounts shall be monitored for potential signs of money laundering and terrorist financing activities. This monitoring shall be done by the Internal Control Group and necessary returns shall be rendered to the CBN and NFIU as at when due.

6.4 RELATED POLICY AND PROCEDURE HANDBOOKS AND MANUALS

- Unity Bank Credit Policy Manual
- Unity Bank Internal Rules.
- Unity Bank Audit & Inspection Manual

- Unity Bank Internal Control Manual
- Operations Manuals & Procedures
- Unity Bank Know Your Customer (KYC) Employee Hand Book
- Unity Bank Whistleblowing Manual
- Unity Bank Employees KYC Handbook
- Unity Bank Board of Directors Charter
- Western Union Anti- Money Laundering and Counter Terrorism Compliance Programme, Policies and Procedures.
- Western Union Operators Duties as regards to the Internal Reporting of Suspicious Transactions
- Unity Bank Anti-Bribery and Corruption Policy

6.5 FUNCTIONS AND RESPONSIBILITIES OF INTERNAL AUDIT IN RELATION TO AML/CFT COMPLIANCE

Internal Audit is an appraisal function established in the Bank to independently examine and evaluate the activities of the Bank as a service to the Board of Directors in particular and to the Management in general. It is a control which functions by examining and evaluating the adequacy and effectiveness of other controls.

Similarly, Section 42.1 of the CBN Anti-Money Laundering / Combating the Financing of Terrorism in Banks and Other Financial Institutions Regulation 2013, as amended requires that "All financial institutions shall make a policy commitment and subject its AML/CFT Compliance programme to Independent testing or require its Internal Audit function to determine the adequacy, completeness and effectiveness of the programme.

To this end, General Audit & Inspection Department is required to carry out periodic review of the Bank's Compliance functions to determine its effectiveness and furnish the Board and the Management with findings and recommendations concerning the Compliance functions.

Internal Audit is also required on an annual basis to review the account(s) of the Chief Compliance Officer and submit a report on findings to the Managing Director.

Internal Audit is required to on a yearly basis (December) render Returns to Central Bank of Nigeria (CBN) and Nigeria Financial Intelligence Unit (NFIU) certification of auditing Compliance functions stating the weaknesses and deficiencies observed and actions taken.

7.0 ANTI-MONEY LAUNDERING AND TERRORIST FINANCING POLICIES, PROCEDURES AND REGULATORY REQUIREMENTS

7.1 Definition of Money Laundering and Terrorist Financing

Money Laundering is a process in which assets obtained or generated through criminal activities are moved or concealed to obscure their link with the crime. Perpetrators of the crime find ways to launder the funds in order to use them without drawing the attention of the applicable authorities.

Money Laundering empowers corruption and organized crime where corrupt public officials and criminals are able to launder proceeds from crimes, bribes, kick-backs, public funds and on some occasion, even development loans from international financial institutions. Organized criminal groups want to be able to launder the proceeds of drug trafficking and commodity smuggling through the financial systems without a trace. In the modern day definition, Money Laundering now covers various predicate offences including child trafficking, prostitution etc. Generally, Money Laundering has three stages:

A. Placement

The physical disposal of cash/property derived from criminal activity. The purpose of this stage is to introduce proceeds into the traditional or non –traditional financial system without attracting attention e.g. purchase of artwork, cash deposits, casinos etc.

B. Layering

This involves separating source of proceeds from ownership by changing the form. This is designed to hamper audit trail e.g. complex wire transfers, resell of assets/properties, opening of several accounts to disguise origin of funds etc.

C. Integration

Re–channeling the laundered funds back to the financial system as legitimate funds. The degree of sophistication and complexity in the money laundering scheme is infinite and is limited only by the creative imagination and expertise of criminals.

Terrorist activities are sometimes funded from the proceeds of illegal activities. Although often linked in legislation and regulation, terrorist financing and money laundering are conceptual opposites. Money laundering is the process where cash raised from criminal activities is made to look legitimate for re-integration into the financial system, whereas terrorist financing cares little about the source of the funds, but it is what the funds are to be used for that defines its scope.

In recent years, the International community has become more aware of the dangers that money laundering and terrorist financing poses in all these areas, and many governments and jurisdictions have committed themselves to taking action. The United Nations and other International organizations like Financial Action Task Force (FATF) are committed to helping governments in any way they can.

7.2 The benefits of adhering to Anti- Money Laundering and Combating the Financing of Terrorism to the Employee and Bank

In adhering to this Manual, as with every aspect of its business, the Bank expects that its Employees will conduct themselves in accordance with the highest ethical standards. The Bank also expects its Employees to conduct business in accordance with applicable

Money Laundering Laws. Bank Employees shall not knowingly provide advice or other assistance to individuals who attempt to violate or avoid Money Laundering laws or this Manual.

Money Laundering laws apply not only to criminals who try to launder their ill-gotten gains, but also to Financial Institutions and their Employees who participate in those transactions. If an employee knows that the property is criminally derived but deliberately fails to make further inquiries, wishing to remain ignorant, may be considered under the law to have the requisite "knowledge".
Bank Employees who suspect money laundering activities should refer the matter to appropriate personnel as directed by their businesses' policies and procedures.
Failure to adhere to this Manual may subject Bank Employees to disciplinary action up to and including termination of employment. Violations of Money Laundering laws also may subject Bank Employees to imprisonment and, together with the Bank, to fines, forfeiture of assets, and other serious punishment.
As a bank, the underlisted policies are put in place to guard against signing on persons and organizations involved in Money Laundering activities:

7.3 Regulatory Framework

Banks are monitored for Money Laundering and Financing of Terrorism activities under the provisions of the following regulations.

7.3.1 List of Regulations

a. Banks and Other Financial Institutions Act 2020 as amended
b. Foreign Exchange Manual 2018
c. Failed Bank Act 1996
d. Corrupt Practices and Other Related Offences Act 2000
e. Economic and Financial Crimes Commission (Establishment) Act 2004
f. Advance Fee Fraud and Other Fraud Related Offences Act, 2006
g. The Nigerian Deposit Insurance Corporation (NDIC), 2006
h. Central Bank of Nigeria Act, 2007
i. Money Laundering (Prohibition) Act 2011 (as amended).
j. Central Bank of Nigeria AML/CFT Regulation 2013 as amended
k. Terrorism (Prevention) Act, 2013
l. Special Control Unit against Money Laundering (SCUML) Regulation, 2013
m. Security and Exchange Commission Code of Corporate Governance for Public Companies
n. The Nigerian Financial Intelligence Unit (NFIU) Act, 2018
o. CBN AML/CFT (Administrative Sanctions) Regulations, 2018
p. Nigerian Code of Corporate Governance, 2018
q. Nigeria Data Protection Regulation, 2019
r. Common Reporting Standards (Regulations) 2019

7.3.2 The Institutions that enforce Compliance with the AML/CFT Regulations.

i. Central Bank of Nigeria (CBN)
ii. The Nigerian Financial Intelligence Unit (NFIU)

iii. The Economic and Financial Crimes Commission (EFCC)
iv. Nigeria Deposit Insurance Corporation (NDIC)
v. Security and Exchange Commission (SEC)
vi. Corporate Affairs Commission (CAC)
vii. Nigerian Customs and Excise
viii. Nigeria Police Force
ix. Special Control Unit against Money Laundering (SCUML)
x. Financial Reporting Council of Nigeria (FRCN)

7.3.3 Under the Money Laundering (Prohibition) Act 2011, Banks are required to render Three reports namely:

a. Section 2 – Duty to report International transfer of funds and securities of value in excess of US$10,000 or its equivalent.

b. Section 6 –Special surveillance of certain transactions (suspicious transactions). The red flag on various types of suspicious transactions are captured in the appendix.

c. Section 10 – Mandatory disclosure by Financial Institutions with a threshold of N5m and N10m for an Individuals and Corporate Bodies respectively.

7.4 Suspicious Transaction/Activity Reporting (STR /SAR).

Suspicious Transaction/Activity) is a transaction/activity that is surrounded by conditions of unusual, unjustifiable complexity or inconsistent with known customer's KYC profile. Section 6 of the Money Laundering Prohibition Act 2011 and Section 13 of FATF 40 Recommendations requires Financial Institutions to submit STR/SAR to the FIU.

Funds with the following characteristics are deemed to be suspicious and should be reported to the NFIU within a period not more than 24 hours immediately upon completion of investigation by Chief Compliance Officer (section 31(3) of CBN AML/CFT regulations 2013);

- are derived from legal or illegal sources but are intended to be used for any act of terrorism and/or;
- are proceeds of crime related to terrorist financing and/or;
- Belong to a person, entity or organisation considered as Terrorist.

When staff detects any "red flag" or suspicious Money Laundering activity, the suspicious transaction/activity should be reported to the Chief Compliance Officer for investigation and reporting. Every action taken on the investigation must be recorded. Bank and its staff shall maintain confidentiality in respect of such investigation and a suspicious transaction report filed with the competent authority. This action is however, in compliance with the provisions of the Money Laundering Law that criminalize "tipping off" (i.e. doing or saying anything that might tip off someone else that he is under suspicion of Money Laundering). The Bank, its Directors, Officers and Employees (permanent and temporary) are prohibited from disclosing the fact that a report is required to be filed with the competent authorities.

The Terrorist Financing Red flags which are not limited to the following are presented below:

a. Persons involved in currency transactions who 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 such as student, unemployed, or self-employed;

b. Financial transaction by non-profit or charitable organisations, for which there appears to be no link between stated activity of the organisation and other parties in the transaction;

c. 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;

d. Where large numbers of incoming or outgoing funds transfer take place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involved designated high-risk locations;

e. Where the stated occupation of the customer is inconsistent with the type and level of account activity;

f. Where funds transferred does not include information on the originator, or the person on whose behalf the transfer is conducted, the inclusion of which should ordinarily be expected.

g. Multiple personal and business accounts or the accounts of non-profit organisation or charities are used to collect and channel funds to a small number of foreign beneficiaries;

h. Foreign exchange transactions which are performed on behalf of a customer by third party, followed by funds transfer to locations having no apparent business connection with the customer or to high-risk countries, and

i. Funds generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from high-risk countries.

When a customer fails to provide information required for a complete due diligence, the bank shall not commence business relationship or shall stop business relationship in the case of an existing customer. A suspicious transaction report shall be rendered to the NFIU in this regard.

Unity Bank shall freeze any account identified to be receiving illicit money transfers and such account's details and mandate shall be submitted to the Nigerian Financial Intelligence Unit and Central Bank of Nigeria. This is in compliance with the Central Bank of Nigeria Circular titled Illicit International Money Remittances Through The Banking System dated August 25, 2016 and reference Ref TED/FEM/FPC/GEN/01/009

Note that Financial Institutions and Designated Non Financial Institutions who carry out their duties under this directive in good faith shall not be liable to any civil or criminal liability nor have any criminal or civil proceedings brought against them by their customers.

The Bank has acquired Soft AML Solution and Soft Watch Filtration Solutions which are for tracking, analyzing and reporting suspicious transactions activities. Once identified, suspicious transactions will be reported to the appropriate Regulatory Authorities.

7.5 Compliance with Legislation

The Bank will observe high ethical standards within the confines of the laws and regulations guiding its operations. In particular, Banks are required to ensure full compliance with the CBN – issued Guidance Notes on Money Laundering Surveillance and the CBN AML/CFT Regulation 2013 as amended in order to enhance the effectiveness of the provisions of the Money Laundering Decree. The Bank is aware of this requirement and will ensure that all its businesses comply accordingly.

7.6 Cooperation with Law Enforcement Authorities

The Bank will give full cooperation to law Enforcement Authorities within the limits of the rule governing confidentiality. For instance, where a Bank is aware of the facts that certain funds lodged in an account was derived from criminal activity or intention, the bank is expected to observe the stipulated procedures for disclosure of suspicious transactions by reporting to the NFIU immediately. The Bank is aware of the need to promptly comply with all requests made in pursuant with the law and co-operate with Law Enforcement Authorities and Regulators by providing required information in their continuous efforts to fight Money Laundering and Terrorist Financing.

8.0 FINANCING OF TERRORISM AND PROLIFIRATION OF WEAPONS OF MASS DESTRUCTION

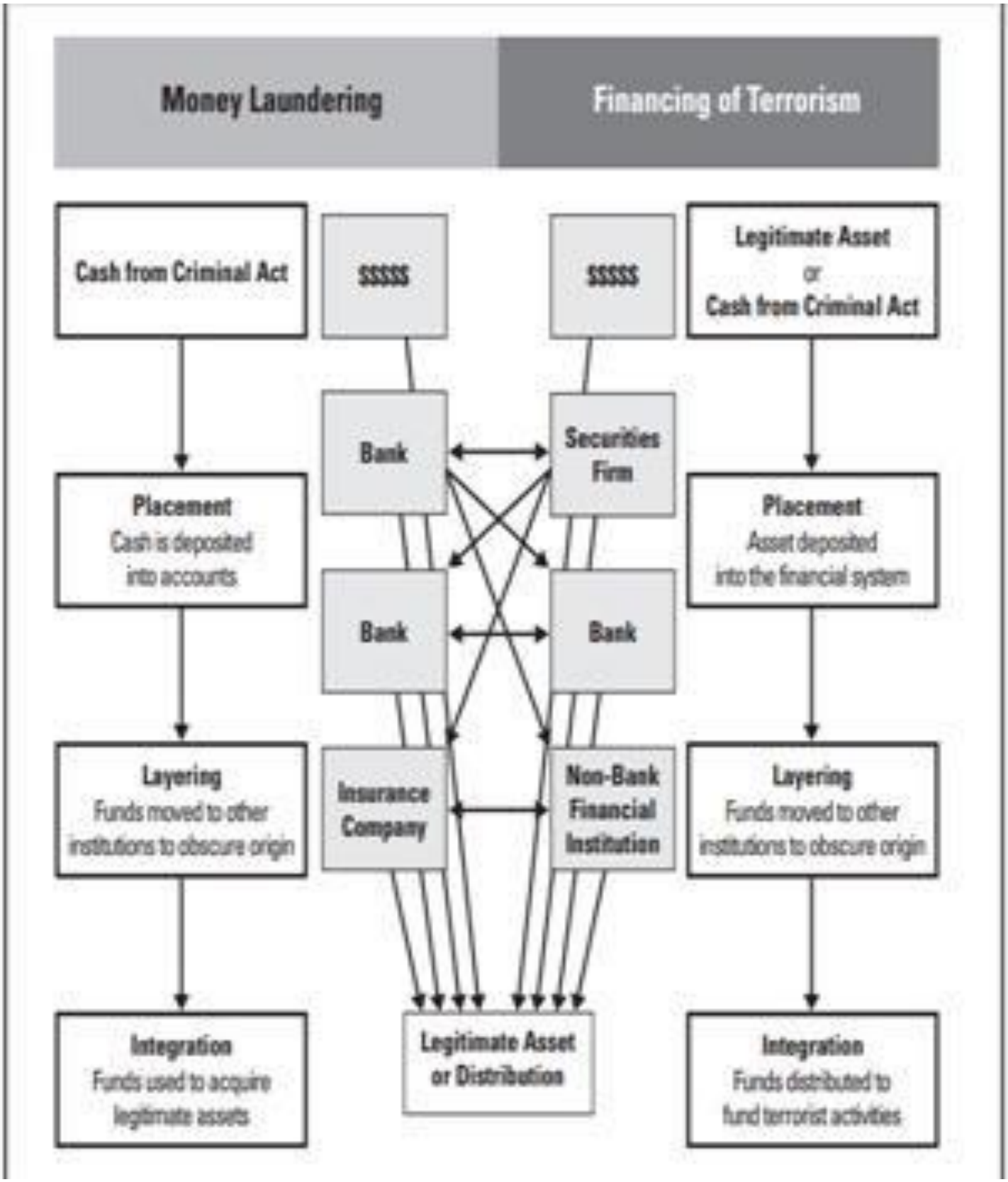
8.1 Terrorism and Terrorist Financing

a) Terrorist Act: Any act intended to cause death or serious bodily injury to a civilian or any other person not taking an active part in the hostilities. Usually, the purpose is to intimidate a population or to compel a government or society to do or abstain from doing any act.

b) Terrorism financing (TF): occurs when a person by any means, directly or indirectly, unlawfully and willfully provides or collects funds with the intention that such funds will be used or in the knowledge that the funds will be used in full or in part, in order to carry out a terrorist act.

c) Terrorist activities are funded from the proceeds of illegal activities. Although often linked in legislation and regulation, terrorist financing and money laundering are conceptual opposites. Money laundering is the process where cash raised from criminal activities is made to look legitimate for re-integration into the financial system, whereas terrorist financing cares little about the source of the funds, but it is what the funds are to be used for that defines its scope.

Difference between Money Laundering and Terrorism Financing illustrated in the figure below:


Money Laundering
Financing of Terrorism
Cash from Criminal Act
Placement
Cash is deposited into accounts
Layering
Funds moved to other institutions to obscure origin
Integration
Funds used to acquire legitimate assets
SSSSS
Bank
Bank
Insurance Company
SSSSS
Securities Firm
Bank
Non-Bank Financial Institution
Legitimate Asset or Distribution
Legitimate Asset or Cash from Criminal Act
Placement
Asset deposited into the financial system
Layering
Funds moved to other institutions to obscure origin
Integration
Funds distributed to fund terrorist activities

8.2 Financing of the proliferation of Weapons of Mass Destruction:

i. The proliferation of weapons of mass destruction (WMD) and their means of delivery such as ballistic missiles are a growing threat to international peace and security. The risk that terrorists will acquire chemical, biological, radiological or fissile materials and their means of delivery adds a new critical dimension to this threat.

ii. Increasing widespread proliferation of weapons of mass destruction increases the risk of their use by terrorist groups and organizations; who could conduct actions aimed at causing large-scale death and destruction.

iii. A transaction may involve a proliferation risk if one or more of the following factors are involved.

iv. The transaction concerns dual-use goods or military goods, whether a license is required or not, and - the goods are destined for a country of concern, and/or - the final destination and end use are not clear, and/or - the client has unusual wishes or conditions in relation to payment, delivery or servicing.

v. Checklist for Dual Goods Transactions:

If a transaction meets two or more of the following conditions, a proliferation risk might be involved:

(i) The transaction concerns dual-use or military goods, whether licensable or not.

(ii) The goods are destined for one of the aforementioned countries of concern. This does not apply, however, to terrorist groups, who do not necessarily operate in or from a country of concern.

(iii) The goods are destined for a transit port that is probably not the end-use location.

(iv) The customer / client is unknown and not prepared to reveal his identity through references.

(v) The customer / client is not familiar with the civilian use of the goods to be delivered.

(vi) The customer / client is vague about end user and end use.

(vii) The customer / client is not or insufficiently prepared to reveal the nature and location of the plant where the goods are to be used or processed

(viii) The customer / client evades answers to normal technical or commercial questions.

(ix) The customer / client is working for or in contact with the defense machinery of a country of concern.

(x) The customer / client demands extraordinary discretion in relation to the order.

(xi) The customer / client offers unusual, favorable terms of payment in proportion to the situation in the country of destination.

(xii) The customer / client demands unusual terms of guarantee.

(xiii) The customer / client is not interested in after-sales service, such as training, installation and maintenance at the end-use location.

(xiv) The customer / client initially agrees to a normal maintenance contract or local inspection arrangement, but dodge it later on.

(xv) The customer / client insists on unconventional conditions for transport and packing.

(xvi) The quantity of the ordered goods differs from a regular civilian use (the quantity may either be unusually big or unusually small).

(xvii) The nature of the customer / client's organization and / or end user does not correspond to the ordered goods.

9.1 PRINCIPLES OF KNOW YOUR CUSTOMER (KYC).

Definition of a Customer

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 (3rd 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 **the Bank**. Example, a wire transfer or issue of high value demand draft as a single transaction.

9.2 Our KYC Standards

The most important means to avoid risks of non-compliance is to have a clear and concise understanding of **"Who the Customer is"** and the **"Nature of his/her business"**

The objective of this Guideline is to prevent the Bank from being used, intentionally or unintentionally for Money Laundering, Terrorist Financing and other Financial and Economic Crimes.

The **KYC** procedures enable the Bank to know / understand its customer and their financial dealings which will in turn help to manage their risks prudently. The **KYC** Policy incorporates the following four (4) elements:

- Customer Acceptance Policy **(CAP)**
- Customer Identification Procedures **(CIP)**
- Risk Management, and
- Monitoring of Transactions **(MoT);**

9.2 ENHANCED DUE DILIGENCE ON SOURCE OF WEALTH/FUNDS

All staff should be vigilant against business entities being used by individuals as a **'front'** for maintaining accounts with banks. Staff should examine the control structure of the entity, determine the source of wealth/funds, the Ultimate Beneficial Owner and identify the natural person who has a controlling interest and who constitutes the management.
Enhanced Due Diligence (EDD) is required for all accounts classified as High Risk. EDD involves obtaining additional documentary evidence for source of wealth/funds, monitoring the account and consistent review of the account.

9.3 CUSTOMER ACCEPTANCE POLICY (CAP)

9.3.1 Criteria for Accepting Customers

The following **Customer Acceptance Policy (CAP)** which indicates the criteria for acceptance of customers shall be followed by the bank:

- ✓ No account shall be opened in Anonymous, Fictitious or Pseudo names

- ✓ Parameters of risk perception shall be clearly defined in terms of the nature of business, location of customer and his/her clients, mode of payments, volume of turnover, social and financial status etc. This will enable categorization of customers into **Low**, **Medium** and **High Risk** which shall be called **Level I**, **Level II** and **Level III** respectively.

- ✓ Customer requiring high level of monitoring for example **Politically Exposed Persons (PEPs)** is categorized as High Risk (Level III).

- ✓ Documents and other information shall be collected from the customer depending on perceived risk and keeping in mind the requirements of the **MLPA** 2011 (as amended) and guidelines issued by the **CBN** and other statutory bodies from time to time.

- ✓ Following appropriate Internal Control Process, an existing account is closed or a new one is not opened where the Bank is unable to apply appropriate **Customer Due Diligence (CDD)** measures. Such may be instances where the staff 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 data/information supplied by the Customer. Staff should

however, ensure that these measures do not lead to the breakdown of relationship with the customer. Where in doubt the **Chief Compliance Officer** of the Bank should be contacted. Furthermore, the customer should be given a prior notice of at least **30 days** and the reasons for closure of the account should also be mentioned.

✓ Concerned staff shall make necessary checks before opening a new account so as to ensure that the identity of the customer does not match those on the **Blacklisted Individuals /Organisations** as per OFAC Portal.

✓ Foreign Operations and International Desk shall invariably consult the Bank's Blacklist Portal and SWIFT Sanction Screening Portal to ensure that prospective persons or Organizations involved in transactions with the Bank are not in any way involved in Terrorist Financing.

9.3.2 Customer Risk Profiling:

A profile shall be prepared for each new customer based on risk categorization**.** The extent and nature of due diligence shall depend on the risk perceived. Staff should bear in mind that the adoption of **Customer Acceptance Policy** and its implementation does not become too restrictive and should not result in denial of banking services to the general public especially to those who are financially or socially disadvantaged.
The Bank has a Solution tagged Customer Risk Profiling Solution which risk rates a prospective customer at onboarding based on the risk criteria provided.

9.4 Risk Assessment

The risk to the customer shall be assigned on the following basis:

9.4.1 Low Risk (Level I)

a. Individuals other than High Net Worth/and entities whose identities and sources of wealth can be easily identified and transactions in whose accounts by and large conform to the known profile may be categorized as low risk. The illustrative examples of low risk customers could be salaried employees whose salary structures are well defined people belonging to lower economic strata of the society whose accounts show small balances and low turnover. government departments and government owned companies, Regulators and Statutory Bodies etc.

b. Public companies (listed on the Stock Exchange or similar situation) that are subject to Regulatory Disclosures
c. Financial Institutions provided they are subject to **AML/CFT** requirements. In all the cases only the basic requirements of verifying the identity and location of the customer shall be met.

9.4.2 Medium Risk (Level II)

Customers that are likely to pose a higher than average risk to the Bank may be categorized as medium or high risk depending on customer's background, nature and

location of activity, Country of origin, sources of funds and Client profile etc.: these include:

a. Persons in business/industry or trading activity where the area of residence or place of business has a scope or history of unlawful trading/business activity.

b. Where the customer profile or the person opening the account, according to the perception of the branch is uncertain and/or doubtful/dubious.

9.4.3 High Risk (Level III)

Staff must apply **Enhanced Due Diligence (EDD)** on such Customers, especially for those where the sources of funds are not clear. The example of customers requiring this higher level of due diligence includes:

a. Politically Exposed Persons **(PEPs)**
b. Financially Exposed Persons **(FEPs)**
c. High Net Worth Individuals (Private Banking Customers)
d. Non-Resident Customers
e. Trusts, Charities, NGOs and Organizations receiving donations
f. Non-Face-To-Face Customers (i.e. offshore accounts)
g. Firms with "Sleeping Partners"
h. Bureau De Change (BDCs)
i. Money Transmission Services
j. Companies that have nominees' shareholders or shares in bearer form

9.5 Red flags at Account Opening Stage

a. A customer exhibits an unusual concern regarding the bank's compliance with government reporting requirements, particularly with respect to his or her identity, type of business and assets, or is reluctant or refuses to reveal any information concerning businesses activities, or furnishes unusual or suspect identification or business documents

b. A customer wishes to engage in transactions that lack business sense, apparent investment strategy or are inconsistent with the customer's stated business/strategy.

c. A customer (or a person publicly associated with the customer) has a questionable background or is the subject of new reports indicating possible criminal, civil or regulatory violations;

d. A customer appears to be acting as the agent for another entity but declines, evades or is reluctant, without legitimate commercial reasons, to provide any information in response to questions about that entity; and

e. A customer has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry.

9.6 CUSTOMER IDENTIFICATION PROCEDURE (CIP)

9.6.1 Background.

Customer Identification means identifying the person and verifying the identity using reliable and independent document such as utility bills or tax receipts or non documentary sources such as visitation or 3rd Party Verification Report. Staff needs to obtain sufficient information necessary to establish, **to their satisfaction** the identity of each new customer whether regular, occasional or walk-in and the purpose of the intended nature of banking relationship.

Being satisfied means the staff is able to satisfy the competent authorities that due diligence was observed based on the risk profile of the customer in compliance with the guidelines outlined in this Manual.

Beside risk perception, the nature of information/documents required would also depend on the type of customer (Individual, Corporate, Trust etc). For customers that are individual persons, the staff shall obtain sufficient identification data to verify the identity of the customer, his address/location, means of identification and recent photograph. For customers that are legal persons or entities, staff shall:

- ✓ Verify the legal status of the entity through search at the **Corporate Affairs Commission (CAC)**

- ✓ Verify that any person purporting to act on behalf of the legal person/entity is so authorized and identify and verify the identity of the person.

- ✓ Unveil the ownership and control structure of the entity and determine who are the natural persons ultimately controlling the entity.

- ✓ Verify that the legal entity exists through address/location confirmation. An indication list of the nature and type of documents/information that may be relied upon for customer identification and verification is hereby given.

- ✓ Where there is no face-to-face contact with a customer and documentary evidence is required, certified true copies by a lawyer, notary public or court of competent jurisdiction, banker, accountant, senior public servant or their equivalent in the private sector shall be obtained provided that the person undertaking the certification is known and capable of being contacted

9.7 Identification and verification of Documentation

S/N	*Account Type/Feature*	*Identification Sources*	*Verification Sources*
1	**Individual Accounts:** ▪ Name ▪ Address	i. Valid International Passport ii. Valid Driver's License iii. National ID iv. Voters Card v. Bank Verification Number (BVN)	▪ Validate identification documents using the Database (online/dedicated platforms) of the relevant ID issuing authorities Utility bill ▪ Tax Receipt ▪ Visitation
2	**Corporate Accounts:** ▪ Legal Status ▪ Principal Place of Business ▪ Mailing Address ▪ Telephone	▪ Certificate of Incorporation ▪ MEMART ▪ Particulars of Director (Form 1.1) ▪ Board Resolution ▪ Power of Attorney ▪ Identification Documents and BVN for Directors and Signatories ▪ Tax Identification Number	▪ CAC Search ▪ Utility Bill ▪ Tax Receipt ▪ Products/Service ▪ Receipt/Agreement / Invoice ▪ Visitation ▪ Verification of TIN
3	**Public Sector Account** ▪ Legal Status ▪ Principal Place of Operation ▪ Mailing Address ▪ Authorized Signatories	▪ Government Edict / Law establishing the institution. ▪ Board Resolution Power of Attorney ▪ Identification Documents and BVN for Directors and Signatories	▪ Collect mandate from DG, commissioner or Minister on authority to open account. ▪ Contact Accountant General of the Federation or of the State where applicable.
4	**Partnership:** ▪ Legal name ▪ Address ▪ Names of Partners and their address ▪ Telephone	▪ Partnership deed ▪ Registration Certificate ▪ Power of Attorney ▪ Identification Documents and BVN for partners and Signatories	▪ CAC Search ▪ Utility Bill ▪ Tax Receipt ▪ Products/Service ▪ Receipt/Agreement/Invoice ▪ Visitation
5	**Trust/Foundations:** ▪ Name of Trustees, Settlers, Beneficiaries and signatories ▪ Name and addresses of the founder, the Managers, Directors and the beneficiaries ▪ Telephone	▪Registration Certificate ▪Power of Attorney Identification for ▪Trustees, Settlers, beneficiaries Resolution of the Managing Body of the Foundation/Association ▪ SCUML Certificate	▪ CAC Search ▪ Utility Bill ▪ Tax Receipt ▪ Products/Service ▪ Receipt/Agreement/Invoice ▪ Visitation
6	**Minor Accounts** ▪ Name of minor ▪ Name of parent/guardian ▪ Address ▪ Parents/**Guardian** Expected Annual Income	• Birth certificate of minor • Valid means of identification and BVN of parent or guardian	▪ Validate identification documents using the Database (online/dedicated platforms) of the relevant ID issuing authorities

	▪ Maximum limit of N20M per transaction		Utility bill ▪ Tax Receipt ▪ Visitation
7	**Refugees and Asylum Seekers** ▪ Refugee Identity Card. ▪ Machine Readable Convention Travel Document (MRCTD)	**Refugee Identity Card**- Issued by National Commission for Refugees, Migrants and Internally Displaced Persons. **MRCTD**- Issued by Nigerian Immigration Service.	• In case of need verification should be done at Nigerian Immigration Service and National Commission for Refugees, Migrants and Internally Displaced Persons.

9.8 Bank Verification Number (BVN)

The Bank Verification Number (BVN) is a centralized biometric identification system for the banking industry, which was launched into the system on February 14, 2014 by the Central Bank of Nigeria.

Unity Bank shall ensure adherence to the Central Bank of Nigeria instructions on the following BVN related matters, as regards the strengthening of the Nigerian Payments System:

(i) Verification of Customers address in account opening.

(ii) Embed BVN biometric data in payment Cards issued to facilitate off-line BVN verification and biometric-based Customer authentication on such Payment Devices as; ATMs, POS, Kiosks etc.

(iii) Approval of BVN Watch-listing modalities and release of necessary Credit Risk Management System (CRMS) data, to facilitate its use for enriching the BVN watch-list.

(iv) Allow Tier 3 Savings Account Customers with BVN and full KYC to deposit cheques **not more than N2,000,000.00 (Two million naira)** in value into their accounts, per customer, per day.

As a result of the various BVN related issues encountered on Customer Accounts, the following clarifications as released by the CBN to all Deposit Money Banks (DMBs) shall guide Unity Bank on BVN related concerns:

1. Correction of wrongly inputted date of birth on BVN record should be allowed **once** with supporting documents evidencing the correct date of birth. (To be verified with the issuing Body)
2. Change of Name due to marriage should be allowed with supporting documents such as marriage certificate/affidavit, etc. (To be verified with the issuing Body)
3. Minor correction of name due to misspelling e.g. Osikoya written as Oshikoya should be allowed with supporting acceptable means of identification showing the correct name.
4. Change of names that are totally different (e.g. Ezra Abu changing to Amina Umar) or partially different (e.g. Ezra Abu Jide to Ezra Abu Olubaje) should be forwarded to Compliance Group for processing. The request should be forwarded along with supporting

documents (Hand written application, Affidavit and Newspaper publication) the documents should also be verified before forwarding to Compliance Group. The request is to be reported to the Nigeria Financial Intelligence Unit (NFIU) by Compliance Group as a suspicious transaction.

5. The Customer's name on the BVN database should be the same in all his/her accounts across the banking industry.
6. Customers that wish to close their accounts should be allowed to do so. Where the account is not linked with the BVN, a payment instrument should be issued in the name in which the account was opened. In cases where the balance on the account is more than what is legally allowed on paper instrument (i.e. N10 million), the bank should seek for and obtain clearance from the EFCC (NFIU) before such accounts can be closed and the balance transferred electronically to another account.
7. Where the bank raises suspicion on the activity of its Customer, Suspicious Transaction Report (STR) shall be filed with the Nigeria Financial Intelligence Unit (NFIU).
8. Timeline for the resolution of BVN issues shall be 5 working days from the date the Customer submits all the required documents.

In line with Central Bank of Nigeria (CBN) Circulars No BSD/DIR/GEN/LAB/12/0021/2/2019- (Linking of BVN Details of All Signatories, Directors and Beneficial Owners to their respective Entity Accounts). The Bank shall ensure all Corporate Customers' accounts have the BVN details of all Signatories, Directors and Beneficial Owners linked to their respective non-individual accounts. This is also mandatory for Non-Resident Non-Nigeria Directors (NRNND) of Corporate accounts. Any non-individual account that does not have the BVN details shall be deemed to have inadequate Know Your Customer (KYC) requirements.

9.9 Dud Cheque Issuance

In compliance with the Central Bank of Nigeria (CBN) Circulars No BSD/DIR/GEN/LAB/08/016- dated 28/6/2016 (Need to implement measures to dissuade issuance of dud cheques in the Nigerian Banking System) the Bank shall on a monthly basis submit a report directly to the licensed Credit Bureaux and the Credit Risk Management System (CRMS) on all Dud cheques issued by a customer whether presented over the counter or through the clearing system for reasons of insufficient funds irrespective of the number of times.
Banks shall on a monthly basis screen all the existing current account customers for purposes of identification of customers who are serial dud cheque issuers.

The Banks shall also continue to perform status check on potential customers on the Credit Risk Management System (CRMS) and from at least two Credit Bureaux before on-boarding a current account customer.

9.10 Account Types

a. Corporate Accounts

All staff should be vigilant against business entities being used by individuals as a **'front'** for maintaining accounts with Banks. Staff should examine the control structure of the entity, determine the source of funds and identify the natural person who have a controlling interest and who constitute the Management.
These requirements may be moderated according to the risk perception e.g. in the case of a public company it will not be necessary to identify all the shareholders. But at least the Promoters, Directors and its Executives need to be identified adequately.

b. Client Accounts

If a Staff has knowledge or reason to believe that a client account opened by a professional intermediary is on behalf of a single client, that client must be identified. Branches may hold 'pooled' accounts managed by professional intermediaries on behalf of entities like Cooperatives, Mutual Funds, Pension Funds or other types of funds.
Branches should also maintain **"pooled"** accounts managed by Lawyers/Chartered Accountants or Stockbrokers for funds held "on deposit" or **"in escrow"** for a range of clients.

Where funds held by the intermediaries are not co-mingled at the branch and there are **"sub accounts"** each of them attributable to a beneficial owner must be identified.
Where such accounts are co-mingled at the branch, the branch should still look through to the beneficial owners. Where the Bank rely on the **"Customer Due Diligence" (CDD)** done by an intermediary, it shall satisfy itself that the intermediary is regulated and supervised and has adequate systems in place to comply with the law requirements.

The Bank shall not open or maintain account for customers such as Wonder Banks, Pyramid Schemes, Ponzi Schemes, Unregistered Money Service (Transmitters) Agents, Shell Banks/Companies and International Businesses and Companies located in high risk Geographical locations and Tax havens.

c. Trust / Charities / NGOs / Foundation / SROs

There exists the possibility that Trust/Nominee or Fiduciary accounts can be used to circumvent the Customer Identification Procedures, the Staff should determine whether the Customer is acting on behalf of another person as Trustee/Nominee or any other Intermediary. If so, the Staff shall insist on receipt of satisfactory evidence of the identity of the intermediaries and if the persons on whose behalf they are acting and also obtain details of the nature of the trust or other arrangements in place.

While opening an account for a trust, Staff should take reasonable precaution to verify the identity of the trustees, and settlers of trust (including any person settling assets into the Trust, Grantors, Protectors, Beneficiaries and Signatories.

Beneficiaries should be identified when they are defined. In the case of a **"foundation"** steps should be taken to verify the Founder/Managers/Directors and the beneficiaries if defined.

d. **Minor accounts**

An account for a minor may be opened by a family member or guardian who is an adult. The identification evidence for that adult who will operate the account shall be obtained in addition to obtaining the birth certificate and passport of the child, provided that strict monitoring shall be undertaken.

Account of a minor shall be constantly monitored to ensure that it is not used for the purposes of money laundering or terrorist financing and that a single transaction does not exceed a limit of 20 million naira per transaction**.**

e. **Online accounts**

Modern technologies have enabled the opening of accounts via the internet. These accounts can be opened either via websites or through mobile phone applications.

Online accounts shall be either for individuals or entities. Online accounts shall be opened with the exact details (i.e., first name, middle name, surname, date of birth, etc.) maintained on customers' BVN.

The KYC requirements for online accounts will be the same for face to face accounts maintained in our branches. KYC documentation may either be obtained via online means or through any of our branches. Measures shall be put in place to confirm that the person opening the online account is the owner of the documents presented. Also, all documents presented shall be verified for genuineness either from issuers databases or via authorized third parties.

Online accounts shall be placed on PND until full KYC is in place. For avoidance of doubt, all online accounts must be maintained on the ICAD portal before debit transactions will be allowed.

f. **Modern Day Slavery/Human Trafficking**

The bank shall not onboard an individual/institution(s) involved in human trafficking, Modern slavery, prostitution or kidnapping activity. Existing customers that are discovered to be involved in such activity shall have their accounts closed down immediately with a report sent to CBN and NFIU.

g. **AML/CFT Compliance with eNaira Transaction**

Unity Bank shall comply with the Money Laundering (Prohibition) Act 2011 (as amended), the Terrorism (Prevention) Act 2011 (as amended) and all subsisting anti-money laundering laws and regulations as may be issued by the CBN from time to time.

We shall monitor transaction through the eNaira portal to ensure that same is not used for terrorist financing.

Unity Bank shall not onboard customer with dormant account, inactive account or account with inadequate KYC.

9.11 Unveiling of Ultimate Beneficial Owner (UBO) of an Account

Section 15 of the CBN AML/CFT Regulations 2013 requires Financial Institutions to take reasonable steps to verify and unveil the identity of a Beneficial Owner to the minimum threshold of 5%. Similarly, the Central Bank of Nigeria via Circular referenced BSD/DIR/GEN/LAB/12/002 dated February 1, 2019 requires Financial Institutions to identify Directors, Signatories and Beneficial Owners of accounts and details of their BVN linked to the entity account.

a. Steps in Identifying Beneficial Ownership

1. Obtain the CAC documents of corporate entities intending to open account;
2. Check the shareholding structure of the company;
3. Confirm the UBO status of the customer (natural/corporate);
4. Conduct due diligence on the shareholders with 5% and above shareholding;
5. Where an entity subscribes to the company and has 5% shareholding and above, its incorporation/registration documents should be obtained;
6. Repeat item 5 above until all individuals linked to the corporate entity are unveiled.
7. Where there exists a complex structure, call for the CAC documents of the corporate shareholders of the entity;
8. Unveil the complex structure and ascertain the natural persons controlling the entity.

b. Some Signs of Account with Ultimate Beneficial Owner

1. Where a phone number not reflected in the account mandate is added to receive transaction alert.
2. Where a signatory to an account always request for more time to come back to the Branch on decisions regarding the operations of the account.
3. When a signatory or shareholder often make reference to another person that is not reflected in the account mandate for decision on running of the account.
4. An individual who is not reflected as either a Director, Shareholder or Signatory to the account but the company pays his household bills (electricity, water, waste, etc.) and domestic staff salaries.
5. A person whose name is not reflected as either a Director, Shareholder or Signatory to the account but often attends Company's business meetings.
6. A Company acquiring assets (Motor vehicles, Generator set, Buildings etc) for an individual who is not reflected as either a Director, Shareholder or Signatory to the account.

7. Where an asset of an individual who is not reflected as either a Director, Shareholder or Signatory to the account is being used to secure facilities for a company or vice-versa

10.0 MONEY LAUNDERING, TERRORIST FINANCING AND BRIBERY & CORRUPTION RED FLAGS MAINTAINED BY THE CHIEF COMPLIANCE OFFICER

Red flags for Money Laundering (ML) and Terrorist Financing (TF) are dynamic and subjective, the underlisted Red Flags therefore are not exhaustive and may be amended from time to time based on emerging trends and typologies as may be observed by the following:

1. The Bank in the normal course of business.
2. Regulators.
3. Law Enforcement and Security Agencies.
4. International and Regional Bodies (e.g. FATF, GIABA etc.).

Similarly, these Red Flags form the basis for the Rules/Model built into the Bank's automated Money Laundering and Terrorist Financing surveillance system.

10.1 Money Laundering (ML) Red Flags

a Accounts that received periodical deposits and are dormant at other periods.

b Accounts opened with the names of the promoters and directors re-occurring in several other accounts in the bank OR individuals serving as company directors for multiple companies headquartered in the same location or sharing the same office.

c Dormant account containing a minimal sum that suddenly receives a deposit(s) followed by daily cash withdrawals until the deposited sum has been withdrawn.

d An account opened in the name of an organization and in which inflows are higher than the nature of business or the income of the prime mover.

e The Opening of multiple accounts by an individual into which numerous small deposits are made that in aggregate are not commensurate with expected income of the customer.

f A dormant account reactivated with an unusually large amount. Large cash withdrawals made from accounts not normally associated with cash transactions.

g Large cash deposits made from accounts not normally associated with cash transactions.

h Split cash lodgment that would have been made in a single transaction using different Tellers.

i The structuring of deposits through multiple branches of the same bank or by groups of individuals who enter a single branch at the same time making deposits into one or separate but linked accounts.

j The deposit or withdrawal of cash in amounts which fall consistently just below reporting thresholds (e.g. CTR - Individual -N5m, Corporate - N10m and FTR - $10,000.00 or its equivalent in other foreign currencies)

k The deposit of multiple monetary instruments at amounts which fall consistently just below reporting threshold especially when the instruments are following sequential order.

l Unrealistic business proceeds or unusual inflows compared to customer's business.

m Sum of debits over previous 30 days greater than Wire Transfer ordered in small amounts in apparent efforts to avoid triggering identification or reporting requirements.

n Transactions involving foreign or local currency that is followed within a short time by wire transfers from areas of concern.

o A business account through which a large in-flow and out-flow wire transfers take place and for which there appears to be no logical business or other economic purpose, especially when such transfers are from or to places of concern.

p Sum of credits over previous 30 days greater than stated occupation of the customer not commensurate with the level or type of activity.

q When opening an account, the customer refuses to provide information required by the financial institution or attempts to reduce the level of information required to the minimum or provide information that is misleading or difficult to verify.

10.2 Financing of Terrorism (FT) Red Flags

i. Persons involved in currency transactions who 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 such as student, unemployed, or self-employed

ii. Financial transaction by non-profit or charitable organizations, for which there appears to be no link between the stated activities of the organization and other parties in the transaction

iii. 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

iv. Where large numbers of incoming or outgoing funds transfer take 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.

v. Where the stated occupation of the customer is inconsistent with the type and level of account activity

vi. Where funds transfer does not include information on the originator or the person on whose behalf the transfer is conducted, the inclusion of which should ordinarily be expected

vii. Multiple personal and business accounts or the accounts of non-profit organizations or charities are used to collect and channel funds to a small number of foreign beneficiaries

viii. Foreign exchange transactions which are performed on behalf of a customer by third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries

ix. Funds generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from high-risk countries.

x. Use of multiple personal or business accounts or the accounts of Non-Profit Organizations or charities to collect and then transfer funds immediately or shortly to a small number of foreign beneficiaries.

xi. Account opened in the name of an individual that is involved in activities that are directly or indirectly related to the activities or claims of terrorist organizations.

xii. Constantly accessing offshore funded accounts via local debit or credit cards.

xiii. Unusual concern for secrecy by a customer, particularly with respect to their identity, type of business, or property held

xiv. Possesses vague knowledge of the amount and detail of a transaction or offers inconsistent or confusing detail about transaction.

xv. Large cash deposit made to the account of an individual or legal entity when the apparent business activity of the individual or entity would normally be conducted in cheques or other payment instruments.

xvi. Mixing of cash deposits and monetary instruments in an account in which such transactions do not appear to have any relation to the normal use of the account.

xvii. Multiple transactions carried out on the same day at the same branch of a financial institution but with an apparent attempt to use different tellers.

xviii. The structuring of deposits through multiple branches of the same financial institution or by group of individuals who enter a single branch at the same time.

xix. The presentation of uncounted funds for a transaction. Upon counting, the transaction is reduced to an amount just below that which would trigger reporting or identification requirements.

xx. The client who transfer several amount overseas along with instructions to pay in cash of non-resident client receive amounts transferred from abroad along with instructions to pay in cash.

xxi. Use of nominees, trusts, family member or third party accounts in an attempt to hide identity.

xxii. Movement of funds through FATF designated non-cooperative countries or territories (NCCT).

xxiii. Deal through intermediaries by delegating/authorizing them to conduct transactions through the account of the suspects or deposit done through them in the accounts of the

suspects or issuing cheques on their behalf or using their accounts in conducting transactions.

xxiv. There is sudden deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.

xxv. When opening an account, the customer refuses to provide information required by the financial institution, or attempts to reduce the level of information provided to the minimum or provides information that is misleading or difficult to verify.

xxvi. An account of which several persons have signature authority, yet these persons appear to have relation among each other (either family ties or business relationship).

xxvii. An account opened by a legal entity or an organization that has the same address as other legal entities or organizations but for which the same person or persons have signature authority, when there is no apparent economic or legal reason for such an arrangement (for example individual serving as company directors for multiple companies headquartered at the same location etc).

xxviii. Wire transfers ordered in small amount in an apparent effort to avoid triggering identification or reporting requirement particularly in location and area under monitoring.

xxix. Wire transfers to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with wire transfer, when the inclusion of such information would be expected.

xxx. Transfers in equal or close values for several persons in different countries or to one beneficiary in several accounts.

xxxi. Avoid direct contact with the bank employees such as constantly dealing through ATM and avoiding the Bank official whenever they try to contact him.

xxxii. Transaction on accounts of community or charitable organizations not consistent with the account profile.

xxxiii. Account opened in the name of a recently formed legal entity and in which a higher than expected level of deposits are made in comparison with the income of the founders of the entity.

xxxiv. Where parties to a transaction (owner, beneficiary etc) are from countries known to support terrorist activities and organizations.

xxxv. Where the individual is included in the United Nations Resolution Council Sanctions list or where they designated under a third country terrorist list or under a Nigeria terrorists designated list.

xxxvi. Purchase of high value goods (e.g precious stones and metal)

xxxvii. The suspect or his representative inquires a lot about the AML/CFT.

xxxviii. The suspect or his representative requests the cancellation of the transaction as soon as the bank employees try to obtain missing important information.

10.3 Bribery and Corruption Red Flags

(a) Offering bribes or inducement by Third parties (Contractors, Consultants and Brokers) to Bank Staff to inflate contracts sum against the interest of the Bank

(b) Corrupt payments made by third-parties (Brokers, Contractors and Consultants) to obtain business from the Bank

(c) Supplier pays a facilitation payment/kickback to an employee of the Bank, to influence the appointment of that supplier

(d) Employee bribes a representative of a supplier, to secure preferential terms on behalf of the Bank

(e) Supplier bribes a third party in order to secure a benefit for the Bank.

(f) Taking advantage by staff (and associated persons interfacing on behalf of the Bank) carrying out Corporate Social responsibilities to seek advantage or reward at the expense of the Bank.

10.4 FINANCIAL INCLUSION GUIDELINES FOR TIERED ACCOUNTS

To further deepen financial inclusion, a three tiered KYC standard shall be utilized. There will be the application of flexible account opening requirements for Tiered KYC low-value and medium value accounts. The low and medium value accounts shall be subject to transaction limitations.

a. Tier 1

A customer would be classified as a TIER 1 client in the instances where the regulatory requirements of Section 46 (2) of the Central Bank of Nigeria AML/CFT Regulations 2013 as amended are met.

In line with the CBN circular dated 1st July 2016 on review of restrictions and limits on levels I and II of the Tiered KYC Accounts, the Tier I account shall be subject to a maximum single deposit amount of N50,000.00 per transaction and maximum cumulative balance of N300,000.00 at any point in time.

The account would also have access to a number of banking transactions within prescribed limits. Such include:

- Mobile Banking Products
- Withdrawals only being performed by the account holder
- Operations only in Nigeria
- ATM withdrawals to a limited amount
- Domestic transactions and no cross-border transactions
- Savings accounts only

b. Tier 2

A customer would be classified as a TIER 2 client in the instances where the regulatory requirements of Section 46 (3) of the Central Bank of Nigeria AML/CFT regulations of the 2013 as amended are met.

In line with the CBN Circular dated 1st July 2016 on review of restrictions and limits on levels I and II of the Tiered KYC Accounts, the Tier II shall be subject to a maximum single deposit amount of N100,000.00 per transaction and cumulative balance of N500,000.00 at any point in time. The account would also operate strictly under caps and restrictions as may be advised by CBN from time to time. Similar to Tier 1 accounts, some of the features of Tier 2 accounts (subject to prescribed limits) include:

- Mobile Banking Products
- Withdrawals only being performed by the account holder
- Operations only in Nigeria
- ATM withdrawals to a limited amount
- Domestic transactions and no cross-border transactions
- Savings accounts only

c. Tier 3

A customer would be classified as a TIER 3 client in the instances where the regulatory requirements of Section 46 (4) of the Central Bank of Nigeria AML/CFT regulations 2013 as amended are met.

There is no limit on cumulative balance, deposit and transactions for TIER 3 accounts.

10.5 SANCTIONS SCREENING (TARGETED FINANCIAL SANCTIONS-TFS)

Sanctions are restrictive measures imposed by competent authorities against countries, persons, groups and/or, legal entities. The extent of the restrictions varies, but most often encompass weapons embargo, entry ban and imposition of freezing of funds and economic resources. In some cases, it may extend to a ban on import and export of products other than weapons.

Unity Bank shall establish the identity of all Customers (prospective and current) with a customer Identity Management System for the purpose of screening customers against the Negative Watch-lists. Also all SWIFT Transfer through the Bank will be scrutinize to determine its integrity. The Soft-Watch AML Filtration solution and SWIFT Sanction Screening has been deployed for the afore-mentioned purpose. Periodic screening is also required to re-verify when changes are made to customers' information or sanctions lists.

All inward and outward wire transfers shall also be screened for possible sanctions using Swift Sanction Screen.

a. Sanctions Lists

Unity Bank recognises the official sanctions list issued by competent authorities. The Bank also recognises any other sanctions regime that may be deemed to be applicable from time to time.

The following official lists are recognised and embedded in the bank's sanctions screening tools:

1. United Nations Security Council (UNSC) List;

   United Nations Security Council Sanctions Lists established pursuant to UNSC Resolutions.

2. United States Office of Foreign Assets Control (OFAC) List;

   The Office of Foreign Assets Control Specially Designated Nationals list and any other targeted Sanctions Lists administered by OFAC.

3. United Kingdom's Her Majesty's Treasury (HMT) List;

   Her Majesty's Treasury Consolidated List of Financial Sanctions Targets in the United Kingdom.

4. European Union (EU) List;
5. CBN and NFIU lists

The Consolidated List of Persons, Groups and Entities Subject to European Union Financial Sanctions.

Note: - It is a serious breach of Account Opening procedure to open or continue business transactions with any customer without proper screening with Filtration solution and all SWIFT Transfer must be screen before consummating same. Defaulters will be sanctioned appropriately

10.6 RISK MANAGEMENT

Unity Bank's KYC policies and procedures cover Management oversight, systems and controls, segregation of duties, training and other related matters.

For ensuring effective implementation of the Bank's KYC Policies and Procedures, the Branch Service Managers (BSM) shall explicitly allocate responsibilities within the Branch.

The Branch shall prepare Risk Profiles of all their existing and new Customers and apply AML/CFT measures keeping in view the risks involved in transaction and account or banking/business relationship. Risk Profiling should be done at different phases of the relationship with the customer.

a. **Assessment of High Risk Customers**

High-risk customers are likely to exhibit one or more of the following characteristics:

- ✓ Politically/Financially Exposed Persons (PEPs/FEPs).
- ✓ Non Governmental Organisation (NGOs).
- ✓ Corporate entities that are owned or controlled by such persons.
- ✓ Designated Non Financial Businesses and Professions (DNFBPs)

The **Know Your Customer (KYC) and Anti Money Laundering Policy** of the Bank therefore, emphasizes the need to exercise due diligence in opening and allowing transactions on accounts for Politically Exposed Persons (PEPs), Financially Exposed Persons (FEPs) Non-Profit Organizations and Non-Governmental Organizations (NGO) within the Bank. Specifically, PEP, FEP, NPO and NGO are classified as high risk and will require special approval for account opening and monitoring of transactions over them.

The PEPs, FEPs, NPO and NGO can pose unique reputational and other risks to the Bank through involvement in the proceeds of corruption, embezzlement, and other illicit activities. Therefore, on an ongoing basis, account holders are monitored to identify those who may have come within the definition of a public figure. Such accounts are identified to enable proper classification as High Risk accounts. Both the CBN and Financial Action Task Force (FATF) emphasized that Financial Institutions in addition to performing normal due diligence measures, should have appropriate risk management systems to determine whether the customer is High Risk. **Also, Executive Director/Zonal Head's approval must be obtained before establishing or continuing relationship with PEPs and FEPs while NPOs and NGOs which are part of Designated Non-Financial Businesses and**

Professions (DNFBPs that are monitored by Special Control Unit against Money Laundering (SCUML) are to be approved by Regional Manager. Branches should therefore, ensure that appropriate approval for opening of such accounts or continuing relationship with them must be obtained using the Enhanced Due Diligence (EDD) Form. Also reasonable measures should be taken to establish the source of wealth and source of funds of such customers.

10.7 Politically Exposed Persons (PEPs)

The CBN AML/CFT Regulation 2013 define **PEPS** as individuals who are or have been entrusted with prominent public functions both in Nigeria and foreign countries and those associated with them. From recent history, it is evident that public office in any of the three tiers or levels of government in Nigeria presents an increasing danger of money laundering and the associated risks. Accordingly, it is imperative to provide a framework for assessing and processing the applications of all persons, natural and artificial, desiring to commence a banking relationship with the Bank as well as the modalities for conducting the relationship, if any.

A Politically Exposed Person includes an individual who either occupies or has occupied a senior position in the Government of the Country, State or Local Council or in a Political Party, Government owned Corporation or in the Armed Forces, Judiciary or the Police.

All senior officials, as defined in this manual, from the three tiers/levels of government (National, State & Local Government), political parties in Nigeria, and related individuals and companies in which these individuals have substantial equity interest or controls are designated public figures.

All accounts maintained by persons who are within the category of Politically Exposed Persons are designated PEP Figure accounts. Every PEP account is designated high risk for Anti-Money Laundering purpose and therefore, requires a higher level of monitoring as indicated below under account monitoring

Care should be taken in dealing with Politically Exposed Persons (PEPs) as contained in the CBN AML/CFT Regulation 2013 and the Financial Action Task Force (FATF) 40 Recommendations of 2011.

The enlarge definition of PEP is individuals with High Public Profiles and their immediate family members. PEPs are individuals who are or have been entrusted with prominent public functions both in foreign Countries as well as in Nigeria. Unity Bank considers anybody that fits this description as High Risk Customers and the following procedures should be followed when dealing with them.

- Conduct Enhanced Customer Due Diligence (EDD).
- Obtain Executive Director/Zonal Head approval.
- Monitor Account Transactions.

There is no duration of time once an individual becomes PEP he or she remains PEP for their entire life and should be treated as such. However, special cases will be determined by the Chief Compliance Officer depending on the risk assessment report on that person.

10.7.1 Domestic and Foreign Politically Exposed Persons (PEPs)

- Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

- Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

- In addition to performing normal Customer Due Diligence measures, the following activities are to be conducted when onboarding a foreign politically exposed person(PEPs) (whether as customer or beneficial owner):

a) Have appropriate risk-management systems to determine whether the Customer or the beneficial owner is a politically exposed person.

b) Obtain approval for establishing (or continuing, for existing Customers) such business relationships.

c) Take reasonable measures to establish the source of wealth and source of funds.

d) Conduct enhanced on-going monitoring of the business relationship and in the event of any transaction that is abnormal; FIs are required to flag the account and to report immediately to NFIU.

We shall take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a Person who is or has been entrusted with a prominent function by an International Organisation. In cases of a higher risk business relationship with such persons, financial institutions should be required to apply the measures referred to in paragraphs (b), (c) and (d).
The requirements for all types of PEP should also apply to family members or close associates of such PEPs. **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.

10.7.2 Nature of PEPs:

PEP accounts are usually basic transactional accounts (LCY and FCY current accounts, etc), personal investment accounts or family owned concerns, with single product need – investments (Time deposits, Treasury bills, Bankers Acceptances or Commercial Papers). The list of public figures is regularly updated and annually approved by the Chief Compliance Officer. The report highlights all transactions within the Bank with amounts over pre-defined limits. Accounts officers are required to review these transactions to ensure they are in line with the customer's profile.

10.7.3 Checklist for Politically Exposed Persons (PEPs)

Identifying Politically Exposed Persons can be a difficult task, particularly, if the customer fails to provide important information or even gives false information. Despite all the Banks' efforts at recognizing Politically Exposed Persons, it is a fact that they do not have the necessary powers, means nor information at their disposal to detect such persons, hence Banks are restricted in what information they can obtain. Compliance Group maintains consolidated list of PEPs. However, it is not exhaustive as Business Directorates are expected to identify PEPs in their locality and update Compliance Group.

10.8 Financially Exposed Persons (FEPs)

A Financially Exposed Person (FEP) is an individual who is a high Level Executive at a Management or Director position in a private Organization. Such clients generally have very high salaries and substantial assets, and are therefore, regarded as Valued Customers.

On their individual capacity, they qualify for enhanced due diligence and will be viewed as Financially Exposed Persons (FEPs).

10.9 Non-Governmental Organization (NGO)

A Non Governmental Organisation is an organisation that is established for the purpose of serving public interest and not for profit making e.g. Nigerian Red Cross Society, Churches etc.

10.10 Bureau De Change

Firms who offer Bureau de change, money transfer or cheque encashment facilities as part of their business operations pose additional risks since such facilities are known to be used by Money Launderers and the Firms concerned may be poorly regulated and have weak or nonexistent KYC procedures. The Bank shall ensure that any Bureau De Change that wishes to conduct business with us, either directly or indirectly has effective AML and Due Diligence procedures in place.

10.11 Designated Non-Financial Businesses & Professions (DNFBPs)

The following are Designated Non-Financial Businesses and Professions (DNFBPs) they are monitored for AML/CFT by Special Control Unit against Money Laundering (SCUML) of Federal Ministry of Trade & Investment which is located in all State Capitals.

Branches should ensure prior to establishing business relationship and continuing relationship with these category of customers obtain evidence of registration with Special Control Unit against Money Laundering (SCUML) of Federal Ministry of Trade & Investment.

These accounts should be closely monitored and reasonable enquiries should be made about transactions passing through the account.

- Dealers in Jewelleries
- Dealers in Precious Metals, Stones, Cars and Luxury Goods
- Chartered / Professional Accountants
- Audit Firms
- Tax Consultants
- Clearing and Settlement Companies
- Lawyers, Notaries and other Independent Legal Practitioners
- Supermarkets
- Hotels / Hospitality Industry
- Estate Surveyors
- Valuers and Real Estate Agents
- Religious and Charitable Organizations
- Casinos
- Pools Betting
- Non-Governmental Organizations (NGOs)
- Non-Profit Organizations (NPOs)
- Trust Companies
- Dealers in Mechanized Farming Equipment and Machineries, Practitioners of Mechanized Farming
- Such other businesses as the Federal Ministry of Trade and Investment or appropriate regulatory authorities may from time to time designate

All transactions that give rise to cause for concern on these accounts should be reported to the CBN and NFIU.

In compliance with the CBN instruction a link has been created under the Application column of the Bank's Portal for branches to key in details of the Registration Certificate submitted by such Customers. Upon keying the Certificates branches should file copy of the Registration Certificate in the Customer's Mandate file.

10.12 Companies that are part of unusual or Complicated Corporate or Trust Structures particularly those that involve several different jurisdictions

This includes International business companies and trusts set up in poorly regulated jurisdictions, particularly those that have limited registration and regulatory requirements including the ability to issue bearer shares where it is often difficult to identify the beneficial owner(s). The Bank would not normally consider establishing a banking relationship with the above type of business due to the difficulty in obtaining sufficient official evidence of ownership. In such cases we must establish that there is a clear and legitimate reason for using such structures.

10.13 Individuals or Firms Based in or Conducting Business with Countries that are Vulnerable to Corruption.

This includes any country where there is a politically unstable regime with high levels of public or private sector corruption.

10.11 Individuals or Firms Based in or Conducting Business with Countries Associated with Terrorist Financing/Drug Trafficking/Production

Individuals or firms who are based in or deal with Countries which are known to be a source of Terrorist Financing including the following:

Afghanistan, Egypt, Iran, Iraq, Israel, Libya, Pakistan, Saudi Arabia, Somalia, Syria, UAE, Uzbekistan, Yemen, Columbia, Caribbean countries, Thailand, Myanmar (formally Burma), Lebanon.

10.12 Individuals or Firms which, in the opinion of Local or Group Management, are considered to be high risk.

Those in these categories are Casinos, Jewellery Sellers, Car Dealers, Oil and Gas businesses, Accountants; Solicitors etc.

10.13 Parastatals, and Organizations that have been created by the Government which aim to contribute to the development of Nigeria.

These are considered high risk because of the possibility of transactions involving the theft of state assets and proceeds of corruption.

10.14 Registered Charities

When dealing with a registered charity, the identity, name and address of the promoters of the charity concerned should be obtained and verified in order to guard against the laundering of fraudulently obtained funds or financing of Terrorism. Accounts for charities in Nigeria are required to be operated by a minimum of two signatories, duly verified and documentation evidence obtained.

10.15 Religious Organizations

A religious organization is expected by law to register with the Corporate Affairs Commission (CAC) and will therefore, have a registered number. Its identity can be verified by reference to the CAC, appropriate headquarters or regional area of the denomination. As a registered organization, the identity of all signatories should be verified.

10.16 Borrowing Customers

In order to minimize the KYC risk involved in the process of facility disbursement to customers, the bank ensures that a proper KYC profile of the borrowing customer is put in place and included in the Credit Report. This is to ensure that facilities are given to customers whose identities are clearly defined and also confirms that Account Officers have displayed knowledge of the customer's business and profile to a reasonable and acceptable risk level.

10.17 Non-Face-To-Face Customers (Offshore Account)

These are Nigerians in Diaspora and others wishing to establish banking relationship but cannot visit the branch, there must therefore be specific and adequate procedures to mitigate the higher risk involved.

Certification of all the documents presented shall be insisted upon and if necessary additional documents may be called for.
In this case of cross-border customers, there may be the need to involve a 3rd Party Verification Company authorized to carry out such exercise by the CBN or SEC.

10.18 Other High-Risk Individuals or Business Types

These are Individuals or Firms who are or have been involved in any of the following:

- Unregulated investment or banking schemes, including pyramid selling.
- The manufacture or sale of armaments.
- The extraction, refining, shipping or sale of Oil and Gas or related products
- Dealing with dangerous, radioactive or toxic substances which may carry substantial human or environmental risks.
- Individuals who have been accused or convicted of a serious crime.
- Individuals who have been directors of insolvent companies or made personally bankrupt.
- Individuals where a professional advisor, regulator or trusted contact has expressed concern.

- Individuals whose business or source of wealth involves activities susceptible to money laundering (e.g. casinos, gambling, nightclubs).
- Places of worship, Charities, Clubs and Societies

11.0 CONSOLIDATED ML/TF RISK MANAGEMENT

Money Laundering and Terrorist Financing poses numerous risks to Banks. Unity Bank shall manage its Money Laundering and Financing of Terrorism risks according to the following guidelines:

11.1 Compliance and Legal risk

This is the risk the bank faces as result of violation of laws, rules, and regulations designed to prevent ML/TF. Such violations could result in fines, civil financial penalties, payment of damages, or litigation of various kinds.

11.2 Operational or Transaction risk

This arises when fraud and errors are not successfully controlled. The consequence is an adverse effect on the bank's ability to deliver its products and services. The risk can arise in any product that can be used to launder money or finance terrorism. Such products and services that are highly vulnerable to ML/TF are deposit-taking, lending, correspondent banking activities, electronic banking processes, and many others.

The Bank's Internal Control as well as Employee Policies and procedures are expected to control this risk.

11.3 Reputation risk

Adverse and negative publicity on the bank due to compliance and legal risks could result in reputation damage of the bank. It must be noted that bank's ability to service existing relationships or to establish new ones is easily damaged by adverse publicity and opinions. Every Staff, and indeed Relationship Managers, must therefore, exercise caution when transacting business with customers and when dealing in business with customers from locations known for high ML/TF vulnerability.

11.4 Credit risk

This risk usually occurs in all lending activities. It is the risk associated with customers' inability to repay borrowed funds from the bank. When credits are extended to customers engaged in criminal activities, overall credit risk becomes substantially high. This is because Money Launderers and Terrorism Financiers do not usually have good intention for the Bank. An appropriate and effective customer acceptance policy is critical to controlling credit risk to the bank.

11.5 Liquidity risk

This can occur as a result of reputation risk on the bank (If the bank is linked with ML/TF) and the resultant withdrawal of public funds. An increase in Liquidity risk occurs when the bank is no longer able to meet its obligations as they come due without incurring unacceptable losses.

11.6 Money Laundering and Financing of Terrorism Risk Assessment Process

The bank is exposed to criminal threats such as Smuggling, Drug Trafficking, Bribery and Corruption, Tax Evasion, Advanced Fee Fraud ('419') and other Economic and Cyber crimes.

The bank adopts risk-based approaches that are commensurate with the specific risks of Money Laundering and Terrorist Financing. Higher Money Laundering risks demand stronger controls than warranted by Individuals or Countries deemed to be of lower risk.

However, all categories of risk whether low, medium or high must be mitigated by the application of applicable controls as provided in this Manual, such as verification of customer identification, Know Your Customer (KYC) policies etc. The ensuing paragraphs provide a framework for identifying the degree of potential ML risks associated with specific customers and transactions in order to ensure focused monitoring of those customers and transactions that potentially pose the greatest risk of ML/TF.

11.7 Identifying Specific Risk Categories

Attempts to conduct illegal activities through the bank may come from sources such as Products, Services and Customers. Also Geographic locations in which the Bank operates may be particularly vulnerable or may have been historically used by criminals for ML/TF activities.

The following specific Products, Services, Customers, Entities and Geographic locations are identified as having ML/TF risk to the bank:

11.8 Products and Services

In evaluating the ML/TF risk with respect to Products and Services, the following becomes relevant:

- Does a particular product or service, new or current?

- Have high transactions or investment value involve international transaction?
- Allow payments to third parties?
- Have unusual complexity?
- Require government verification of customer eligibility?
- Allow the customer to be treated anonymously?

These categories of transactions include electronic funds payment services 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.

Others types of transactions includes;

- 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 through accounts (PTA); 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.

11.9 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. 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 customer that has a history of involvement in criminal activities should receive the highest ratings. Political figures or those in political organizations should score toward the top of the 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 customer types, though not exhaustive, indicates the customers and entities that are likely to pose a higher level of risk to the bank. The Bank shall ensure that Enhanced Due Diligence (EDD) is conducted and Senior Management approval obtained before any form of relationship is established with such customers.

- ✓ Foreign Financial Institutions, including Banks

- ✓ Foreign Money Services providers
- ✓ Bureau de change
- ✓ Private Investment Companies (PICs)
- ✓ Politically Exposed Persons (PEPs)
- ✓ Financially Exposed Persons (FEPs)
- ✓ Non-resident Aliens and Accounts held by Foreign Individuals
- ✓ Cash intensive Businesses (Restaurants and Fast Food Businesses, Liquor Stores)
- ✓ Large Merchandise Distributors
- ✓ Car and Petroleum Dealers.
- ✓ 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

Such variables as the customer type, geographical location, Product and Services and Channels of delivery should be considered to accurately assess customer's risk. For the purpose of this Manual, the following section details the variables to be considered in assessing ML/TF risks of various categories of customers of the bank.

11.10 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 located in countries with higher risk of Money Laundering and Terrorist Financing.

When looking specifically at money laundering risk with respect to customers' location of business or residence, 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.

- ✓ United States Office of Foreign Assets Control
- ✓ The United States Financial Crimes Enforcement Network,
- ✓ European Union, World Bank, the United Nations Security Council Committee,
- ✓ Central Bank of Nigeria (CBN) sanctions list, etc.
- ✓ Whether the Country is or has been on the Financial Action Task Force's (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 issues are overall reputation of the Country 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's 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 Chief Compliance Officer.

11.11 Analysis of Specific Risk Categories

The next stage of the risk assessment process is the analysis of data obtained during the risk identification stage so as to accurately assess ML/TF risk accurately.

Evaluation and analysis of data pertaining to the bank's activities should be considered in relation both to the bank Customer Identification Program (CIP) and to Customer Due Diligence (CDD) information. For the purpose of this Manual, analysis of customers' data and account profile should specifically take into account, 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.
- ✓ Method of opening account
- ✓ Identification used
- ✓ Nationality
- ✓ Customer address information
- ✓ Residency status
- ✓ Beneficiary owner

11.12 Risk Categorization of Products

Unity Bank shall consider all accounts, credit products and other services and determine the level of risk the Bank is exposed to when making them available to its customers (legal and natural).

The risk rating of the products and services shall be based on the prior experiences, type of documentation required from the customers for each product and service and account monitoring platform put in place by the Bank.

11.13 Measurement of Money Laundering / Financing of Terrorism Risk

Unity Bank has adopted a risk based approach by identifying the criteria to measure potential Money Laundering risks. Identification of the Money Laundering risks of customers and transactions will allow the Bank to determine and implement appropriate measures to mitigate these risks.

Unity Bank shall measure its Money laundering risks using the following risk criteria:

a) Country risk

b) Customer risk

c) Products risk

d) Services risk

e) Delivery channel risk

f) Location / Jurisdiction risk

Unity Bank shall attach weight to these risk categories (individually or in combination) in assessing the overall risk of potential money laundering and financing of terrorism. The application of these risk categories is intended to provide a strategy for managing potential Money Laundering risks associated with potentially high risk customers.

11.14 Review of Risk Assessment Approach - Applicability to Existing Customers

Unity Bank shall consider, depending on the on-going relationship whether a risk assessment should be carried out in respect of existing customers. If the Bank is satisfied with its existing risk control measures for a particular customer, additional risk assessment may not be considered necessary.

Any decision in this regard shall be taken in the context of the overall risks of the Bank's business or events with respect to particular customer’s transactions or business lines that become apparent through monitoring of transactions.

11.15 Risk Variables

Unity Bank shall adopt a risk-based approach in determining the level of risk a particular client represents to the Bank. The risk based approach methodology shall also take into account additional risk variables, specific to any particular customer or transaction. These variables may increase or decrease the perceived risk posed by a particular customer or transaction.

Unity Bank shall consider the following risk variables in its risk assessment approach:

- The level of assets to be deposited by the particular customer or size of transactions undertaken. Unusually high level of assets or unusually large transactions compared to what might reasonably be expected of customers with a similar profile may mean that customers not otherwise seen as higher risk should be treated as such. Low levels of assets or low value transactions involving customers that would otherwise appear to be higher risk mean that the Bank may decide to treat such customers as lower risk within an overall risk based framework.

- The level of regulation or other oversight or governance regime to which a customer is subject. A customer that is a Regulated Financial Institution in a jurisdiction recognized as having adequate Anti-Money Laundering ('AML') standards poses less risk from a Money Laundering and Terrorism Financing perspective than a customer that is unregulated or subject to minimal AML regulation. Other companies and their wholly owned subsidiaries that are publicly owned and traded on a recognized Stock Exchange pose minimal Money Laundering risks. These entities may not need to be subjected to as stringent account opening due diligence or transaction monitoring during the course of the relationship.

- The regularity or duration of the relationship. Long standing relationships involving frequent client contact throughout the relationship may present less risk from money laundering perspective. The familiarity with a jurisdiction, including knowledge of local laws, regulations and rules, as well as the structure and extent of regulatory oversight, as a result of the bank's operations within the jurisdiction. Greater familiarity will enhance the ability of the Institution to assess the client. The use by clients of intermediate corporate vehicles or other structures that have no clear commercial or other rationale or that unnecessarily increase the complexity or otherwise result in a lack of transparency for the Bank. Such vehicles or structures will increase the risk unless the rationale is understood and the structure is sufficiently transparent to the Bank.

- Measures and Controls for Higher Risk Situations. Unity Bank shall design and implement appropriate measures and controls to mitigate the potential Money Laundering and Terrorism Financing risks of those customers that are determined to be higher risk as a result of the Bank's risk assessment process. Such measures and controls may require investment both in terms of resources and time in order to identify and capture appropriate customer risk data. Unity Bank shall take the following measures and controls to reduce the risks:

    - Increased awareness of higher risk situations within business lines.
    - Increased levels of Know Your Customer ("KYC") or Enhanced Due Diligence.
    - Increased Monitoring of Transactions and

- Increased levels of Ongoing Controls and reviews of relationships.

11.16 Customer Risk Assessment Matrix

In order to improve the monitoring and control process of our client base, the bank shall categorize its customers by their perceived risk rating – either: **HIGH, MEDIUM or LOW** risk using the Risk Assessment Matrix below where **1 Low Risk 2 Medium Risk and 3 High Risk.** The below customer risk assessment process is automated

Account Opening Method	**Risk Level**		
	1	2	3
In person, all parties present	√		
In person, less than all parties present		√	
Mail/Post			√
Telephone/E-mail			√

Identification Used	**Risk Level**		
	1	2	3
National ID card	√		
Nigerian passport	√		
Driving license	√		
Proxy	√		
Others (as approved by Bank's Management)		√	

Nationality	**Risk Level**		
	1	2	3
Lebanese, Indians, Russian, South America & old Soviet Republics, Nigerians			√
South East Asia (e.g. Thailand, Indonesia, Philippines), South West Asia (e.g. Afghanistan, Pakistan), Africans (except Nigerians)		√	
All others	√		

Customer Address Information	**Risk Level**		
	1	2	3
Within locality	√		
Within state		√	
Within country			√
Outside country			√

**If existing customer and no new accounts have been opened, then assign 1 to risk level indicator

Residency Status	**Risk Level**		
	1	2	3
Resident	√		
Non-resident			√

Beneficiary / Owner	**Risk Level**		
	1	2	3
If customer is acting as an agent for non-resident beneficiary			√
If customer is acting for resident beneficiary		√	
If customer is actual owner	√		

Purpose of the Account	**Risk Level**		
	1	2	3
Salary	√		
Saving	√		
Business		√	
Others			√
Type of Products or Services Chosen	**Risk Level**		
	1	2	3

Any/all of the following: Electronic funds payment services Electronic Banking Foreign Exchange and funds transfers Domestic and international private banking Foreign correspondent accounts, such as payable through accounts (PTA); foreign currency denominated accounts. Trade finance or letters of credit Lending activities, particularly loans secured by cash collateral and marketable securities			√
Other type of products/service	√		

Source of Funds / Countries Doing Business With	**Risk Level**		
	1	2	3
FATF list			√
Other countries	√		

Nature of Business	**Risk Level**		
	1	2	3
Businesses in: currency exchange, investment brokers, leather goods store, car dealers, travel agencies, jewel & gem dealers, import/export, cash intensive businesses such as restaurants and retail stores hotels and furnished apartments, government contractors. Casino			√
Businesses in: charity organizations, professional service providers (lawyers, accountants, etc.)		√	
All others e.g. manufacturing, construction, etc.	√		

Structure of Business*	**Risk Level**		
	1	2	3
Retail			√
Commercial		√	
Corporate	√		
Group accounts			√

Largest Single Transaction*

Largest Single Transaction **"For Individual Accounts"**	RISK LEVEL		
	1	2	3
More than =N=5,000,000			√
More than =N=1,000,000 but less than =N=5,000,000		√	
Less than =N=1,000,000	√		

"For Business Accounts"

Risk Level		
1	2	3
		√
√		

Cumulative Monthly Value of Transactions "For Individual Accounts"**	**Risk Level**		
	1	2	3
More than ₦ 10,000,000			√
More than ₦5,000,000 but less than N10,000,000		√	
Less than ₦ 5,000,000	√		

*If unknown, assign 2 to the risk level

Cumulative Monthly Value of Transactions "For Business Accounts"**	**Risk Level**		
	1	2	3
More than ₦ 100,000,000			√
More than ₦50,000,000 but less than ₦ 100,000,000		√	
Less than ₦ 50,000,000	√		

STEP ONE:

Fill below the risk level matches with your customer & account profile after being compared with the above – mentioned risk indicators.

Risk Indicator	**Risk Level (1, 2, 3)**
a)Account Opening Method	
b)Identification Used	
c)Nationality	
d)Customer Address Information	
e)Residency Status	
f)Beneficiary Owner	

g)Purpose Of The Account	
h)Type Of Products Or Services Chosen	
i)Source Of Funds/Countries Doing Business With	
j)Nature Of Business	
k)Structure Of Business	
l)Largest Single Transaction – Individual	
m)Cumulative Value Of Transactions	
n)Largest Single Transaction – Business	
o)Cumulative Value Of Transactions	
TOTAL	

STEP TWO:

Apply the total number with below conditions

CONDITION	**CUSTOMER RISK**
If Total Equal & Below	***23 Low (Below 50%)***
If Total above 23 & Below	34 Medium (50 – 75%)
If Total Equal 34 and	***Above High (Above 75%)***

**** EXCEPTIONS***

1. If you have assigned eight or more 'risk level 3' indicators (no matter the total score), customer risk will automatically become high risk and involve enhanced due diligence
2. All quoted companies to attract low risk.
3. All staff accounts & spouse accounts to attract low risk.

*** Accounts of Politically Exposed Persons (PEPs) to attract high risk as per CBN guidelines.

*** Elected politicians, Political appointees & Senior Government officials not below the level of Directors.

11.17 MITIGANTS TO ML/TF RISK

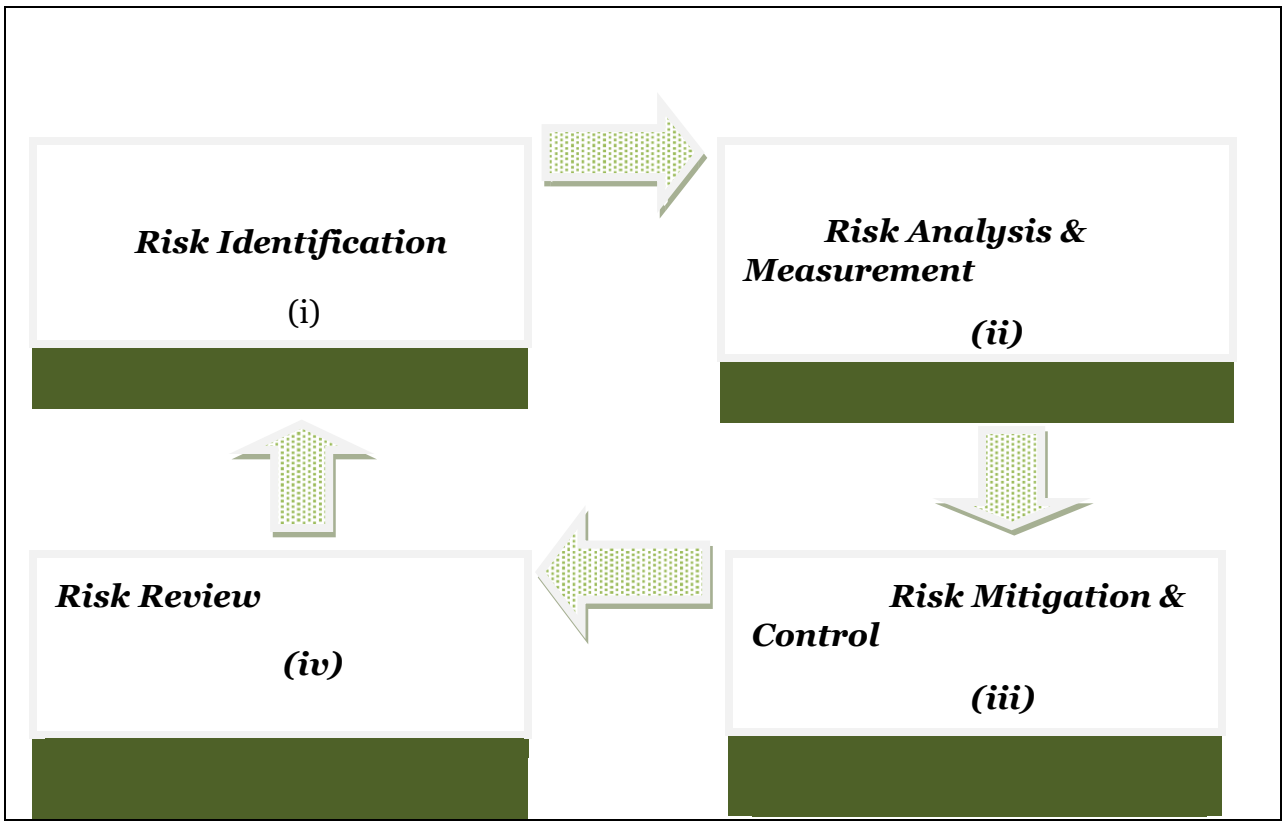
The risks identified suggest the possibility / probability / likelihood that the Bank can be used for Money Laundering & Terrorist Financing.

AML/CFT Compliance risk can be categorized into two (2) namely;

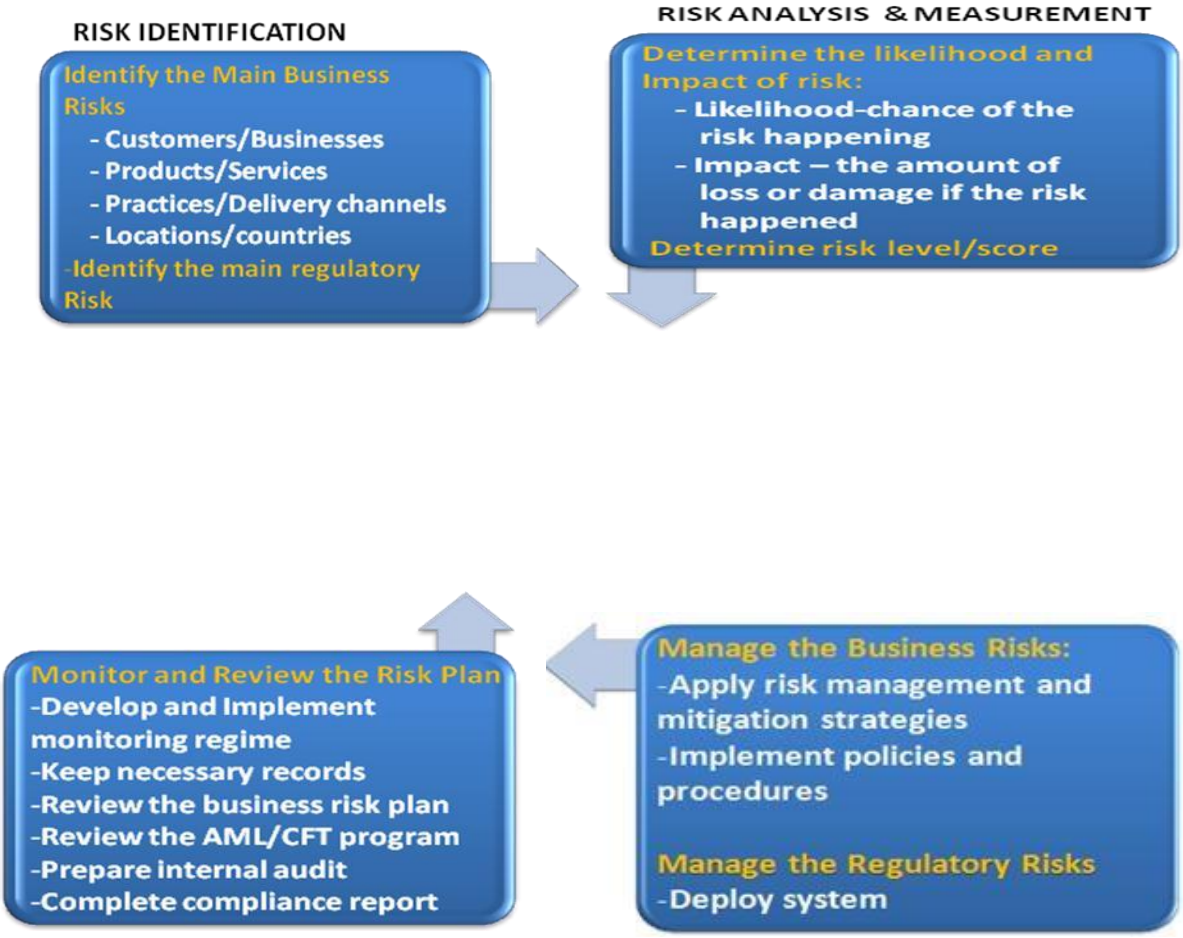
a) Business risks: - These risks are inherent and can be manifested in the way the following are managed;
   (i) Customers
   (ii) Products
   (iii) Services
   (iv) Delivery Channels
   (v) Locations
   (vi) Geography / Jurisdiction
   (vii) Business Practice

b) Regulatory Risks: - This can be manifested as a result of the following;
   (i) Rendition of Statutory Reports
   (ii) Weak Customer Due Diligence / Enhanced Due Diligence Procedures
   (iii) Non -Effective Internal Control
   (iv) Non-Effective Internal Audit functions
   (v) Non-Effective Preventive measures
   (vi) In effective monitoring & detection systems
   (vii) Poor record keeping

Risk Management Flow Chart for Managing Risks:



Our Risk Model:



Our preventive/proactive measures to protect the Bank against being used for Money Laundering and Terrorist Financing are through the followings:

1) Written Program and Policy
2) Management Staff Structure
3) Know Your Customer / Employee Policy
4) Internal Control Mechanism
5) Internal Audit Supervision
6) Customer Due Diligence
7) Simplified Due Diligence
8) Enhanced Due Diligence
9) Monitoring of Customers / Accounts / Transactions

10) Risk Review / Update
11) Mandatory Reporting – Statutory Anti-Money Laundering Reports (vis-à-vis Currency Transaction Report (CTR)/ Foreign Transaction Report, Suspicious Transaction Report
(STR) and others like Risk Based Supervision Reports etc
12) Suspicious Transaction Report Policy
13) Record Keeping / Preservation Policy
14) Implementation of Robust Anti-Money Laundering Solution
15) Risk Management Procedure for Politically Exposed Persons (PEPs) and other High Risk customers
16) Customer Risk Profiling
17) Sanction List Screening Solution
18) Independent Testing / Audit
19) Code of Corporate Governance
20) Code of Professional Ethics
21) Confidentiality & No Tipping Off
22) Whistle Blowing Policy

12.0 CUSTOMER DUE DILIGENCE

The components of Due Diligence covered by this manual include Customer Due Diligence (CDD) Reduced or Simplified Due Diligence and Enhanced Due Diligence (EDD) which shall apply to customer on a case by case basis. Customer Due Diligence includes KYC; Sanctions Screening and Enhanced Due Diligence

Customer Due Diligence shall apply to all prospective customers before account or business relationship is established with the Bank. In Unity Bank, CDD shall constitute the first level check on all documents provided to verify and record the identity of prospective customers, as well as additional information about his background, business, and likely level of activity at the Bank. It shall be a major factor in the Bank's overall AML/CFT control process. CDD is used to verify and record identity of all prospective customers irrespective of the level of risk.

12.1 Reduced or Simplified Customer Due Diligence (CDD)

Where there are low risks, Unity Bank shall apply reduced or simplified measures. In circumstances where the risk of money laundering or terrorism financing is lower, information on the identity of the customer and the beneficial owner of a customer is publicly available or where adequate checks and controls exist elsewhere in national systems, or where the volume transacted in the accounts is considered low.

In the event that the Bank applies Simplified or Reduced Customer Due Diligence measures to customer's resident abroad, it shall be limited to customers in Countries that have effectively implemented the Financial Action Task Force (FATF) recommendations.

The Simplified CDD measures shall not apply to a customer whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios. In such a circumstance, Customer should be subjected to Enhanced Due Diligence

12.2 Enhanced Due Diligence (EDD)

Enhanced Due Diligence is a process that has mandated an increased level of monitoring for customers who are considered high-risk. It goes as far as identifying the beneficial owners of entities and understanding their line of business.

Unity Bank shall perform enhanced due diligence for high risk categories of customer, business relationship or transaction.

12.3 Exemptions from Customer Due Diligence

Unity Bank shall not after obtaining all the necessary documents and being so satisfied repeatedly perform identification and verification exercise every time a customer conducts a transaction

Unity Bank shall ensure that ongoing due diligence is performed based on a customer's assigned risk rating. In this regard, as a minimum, periodic customer reviews must be performed in accordance with the following time periods:

- ✓ High risk: on an annual basis;
- ✓ Medium risk: every two (2) years; and
- ✓ Low risk: every three (3) years.

12.4 Ongoing monitoring

The first requirement of knowing your customer for money laundering and terrorist financing purposes, is for the Bank to be satisfied that a prospective customer is who he claims to be.

The Bank shall not establish a business relationship until the relevant parties to the relationship have been identified, verified, and the nature of the business they intend to conduct is ascertained.

Where an on-going business relationship is established, any activity that is not consistent to the business relationship shall be examined to determine whether or not there are elements of money laundering, terrorist financing or any suspicious activity.

Where a customer is acting on behalf of another in a situation where funds are supplied by someone else or the investment is to be held in the name of someone else, the Bank shall verify the identity of the customer, the agent or trustee except where the customer is itself a Nigerian regulated financial institution.

Unity Bank shall establish and maintain adequate procedures to ensure that all KYC information and supporting documents are reviewed and updated periodically where there is an ongoing business relationship with the customer.

In this regard the following events trigger a need to review customer information

- Periodic review of the customer
- Where the customer voluntarily advises Unity Bank that its KYC information has changed;
- Where an existing customer takes out a new product or opens a new account;
- Where a staff member conducts a review on the customer in the normal course of business and ascertains that the customer information has changed;
- When a transaction of significance takes place;
- When there is a material change in the way an account is operated;
- When Unity Bank becomes aware that it lacks sufficient information about an existing Customer.

The Bank shall take reasonable steps to keep the information up-to-date as the opportunities arise, including where an existing customer opens a new account.

Any information obtained during any meeting, discussion or other communication with a customer shall be recorded and kept in a customers' files to ensure, as far as practicable, that current customer information is readily accessible by the Anti-Money Laundering Compliance Officers (`AMLCOs') or relevant regulatory bodies or law enforcement agencies.

12.5 Approval of High Risk Relationships

Opening of account or continuing relationship with customer that match on a Sanctions List is prohibited. **Account of Politically Exposed Persons (PEPs) and Financially Exposed Persons (FEPs) must be approved by the Executive Director /Zonal Head. Similarly, other High risks Accounts are to be approved by Regional Manager.** The approval/rejection is to be given through duly completed Enhanced Due Diligence (EDD) Form.

12.6 AML /CFT ISSUES IN CORRESPONDENT BANKING AND CROSS BORDER RELATIONSHIP

Correspondent banking is the provision of banking services by one bank (i.e. "correspondent bank") to another bank (i.e. "Respondent bank") These services may include Cash/Funds Management, International Wire Transfers, drawing arrangements for demand draft and mail transfers, payable-through-accounts, cheques clearing etc.

The bank while entering into any kind of correspondent banking arrangement shall gather sufficient information to understand fully the nature of the business of the correspondent/respondent bank. Information on the Bank's Management, major business

activities, level of AML/CFT compliance, purpose of opening the account, identity of any 3rd Party entities that will use the correspondent banking services and Regulatory/Supervisory framework in the correspondent's country.

Similarly, the bank shall also ascertain from publicly available information whether the other bank has been subject to any Money Laundering or Terrorist financial investigation or Regulatory action.
Such relationships shall be established only with the prior approval of the Board. The Bank shall not enter into a correspondent relationship with a "Shell Bank". A shell bank is one which is incorporated in a country where it has no physical presence and is unaffiliated to any regulated financial group. "Shell Banks" are not permitted to operate in Nigeria.
Unity Bank will not establish any relationship with respondent foreign Financial Institution that permits their accounts to be used by "Shell Banks"
Unity Bank shall ensure that adequate and effective controls are in place to avoid the opening of correspondent banking relationships with Shell Banks.
Unity Bank must, in relation to cross-border correspondent banking and other similar relationships, in addition to performing standard CDD, also:

- Gather sufficient information about a correspondent institution to understand fully the nature of the correspondent's business and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether it has been subject to an ML/TF investigation or Regulatory action;
- Assess the Correspondent Bank's AML/CFT controls;
- Clearly understand the respective responsibilities for each institution in respect of the particular arrangement/transaction;
- Confirm whether the Correspondent Bank offers payable through accounts and be satisfied that the Correspondent Bank has conducted CDD on customers who have direct access to accounts of the Correspondent Bank, and that it is able to provide relevant CDD information upon request. In the instance where a Correspondent Bank offers payable-through accounts, these relationships must be escalated to the Chief Compliance Officer for consideration and approval.

Similarly, the Bank shall verify identity of Investors in the Bank where the amount payable is $1000.00 and above or equivalent.

12.7 NEW TECHNOLOGIES AND NON-FACE -TO - FACE TRANSACTIONS

Unity Bank shall ensure that Electronic Card products issuance and Usage are properly monitored to forestall Money Laundering and Terrorist Financing. The Card products shall be subjected to AML/CFT compliance monitoring. The Bank shall conduct regular monitoring of Card products by computerized monitoring systems/solutions that are designed to recognize unusual transactions and related patterns.

AML/CFT Compliance Officers shall review these solutions, record exemptions and report same to the relevant Regulatory Authorities (CBN and NFIU).

12.8 Minimum Standards for Card Issuance and Usage:

As a certified PCI DSS and ISO 27001 Organization; Unity Bank is guarded by the provision of Section 3.11 of CBN guidelines on Card Issuance and Usage (2014); The Bank shall ensure;

That a robust AML/CFT program is in place to prevent Money Laundering and Terrorist Financing using Cards, e-payment or other electronic platforms. The Bank shall therefore ensure the following:

- Complete KYC requirements are obtained before granting access to Customers on any of the Electronics Payment Platforms.
- Appropriate limits are placed on Payment Cards and all indemnity executed
- A robust Anti-Money Laundering Solution is in place to monitor Cards and other electronic payment systems against Frauds, Money Laundering and Financing of Terrorism.
- A comprehensive risk-management framework (including Policy & Procedure for eProducts) is in place to ensure efficient monitoring, management or mitigation of risk emanating from Cards and other electronic payment channels / platforms.
- All payment card transactions are subjected to current Nigerian Financial Intelligence Unit (NFIU) reporting requirements.
- Rendition of all Regulatory Returns in respect of Cards and other Electronic Products.
- Proper AML/CFT training is conducted for all Staff involved in Cards Issuance and Management.

12.9 Specific Requirements for Stored Value Cards (Individual and Corporate)

- No stored value card shall be issued to a person without obtaining the minimum KYC.
- The maximum amount that can be loaded on the stored value card shall not exceed ₦500,000.00 per day.
- The maximum balance on the stored value card shall not exceed ₦500,000.00 at any time.
- The limits specified for stored value cards shall also apply to cards linked to Mobile Money Wallets, where least KYC (Phone Number and Name) has been performed on the Mobile Money Customer.

12.10 Specific Requirements for Prepaid Cards (Individual and Corporate)

- Prepaid cards issued shall operate at least within the minimum KYC requirements prescribed by the CBN. However, loadable limits (in Naira and Foreign currency) and daily balances shall be as per our relevant policy.

- No prepaid card shall be issued beyond the limits of a stored value card to a person or a Corporate Organization. Where a customer desires to do transactions beyond the limits prescribed above, full KYC would be required.

12.11 Specific Requirements for Debit Cards

- Debit cards shall be issued to customers having Savings and Current Accounts with full KYC requirements of their respective categories.

12.12 Specific Requirements for Credit and Charge Cards (Individual and Corporate)

- An issuer should identify sources of credit risk, routinely measure and monitor credit exposures, and use appropriate risk-management tools to control these risks and minimize credit and charge cards defaults.

13.0 TRADE BASED AML/CFT/CPF COMPLIANCE:

Trade-based Money Laundering is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. In many cases, this can also involve abuse of the financial system through fraudulent transactions involving a range of money transmission instruments, such as wire transfers.

✓ Trade Based Money Laundering, Terrorist Financing and Proliferation Financing.

Trade Based ML and TF was recognized by the Financial Action Task Force (FATF) as one of the main methods by which Criminal Organizations and Terrorist Financiers move money for the purpose of disguising its origin and integrating it back into the formal economy. It is a very complex method as it involves national borders.

Banks facilitate global trade by offering various financial products (e.g. Letters of credit, guarantees, etc.) and thus banks play a vital role in mitigating the risk associated with Trade Based Money Laundering and Terrorist Financing in order to effectively minimize this risk.

✓ Trade Misinvoicing

Trade Misinvoicing is not only the most significant form of trade based Money Laundering and Terrorist Financing but also the largest component of illicit financial outflows and is used for the following reasons.

- Money Laundering, Terrorist Financing and Proliferation Financing
- Evading Taxes
- Evading Customs Duties
- Claiming Tax Incentives
- Dodging Capital Controls

13.1 Common Techniques in Trade Misinvoicing

The following are some of the common Techniques in Trade Misinvoicing:

- **Over-invoicing**

Enables the importer to transfer value to the exporter. Trade goods are invoiced at a price above the fair market price, the exporter then transfer value from the importer as the payments for the trade goods which will be higher than the fair market value of goods the exporter has sent.

- **Under-invoicing**

Enables the exporter to transfer value to the importer at a price below the fair market price-the importer then transfer value to the exporter as the payment for the trade

- **Multiple Invoicing**

A Money Launderer or Terrorist can justify multiple payments for the same shipment with more than one invoice for the same international trade transaction, which will enable the Money Launderer or Terrorist financier to justify multiple payments for the same shipment.

- **Over and Under-Shipment**.

Most extreme case is "Phantom Shipments "the quantity of goods shipped relative to the payments sent/receive will be discovered to be overstated or understated.

- **False Description of Trade Goods**

Misrepresenting the quality or type of the goods. The quality or type of the trade goods is misrepresented.

- ✓ **Common situational or behavioral Red Flags in Trade Finance**

The following are Red flags that may be present in every step of the Trade Finance process, which should be promptly examined to detect elements of Money Laundering and Terrorist Financing. Although it is not necessarily an indicator of criminal activity, the presence of a Red Flag requires thorough investigation, in order to properly determine if unlawful acts were committed. For the purpose of detecting ML/TF activities due diligence must be conducted on Customer, Country of origin, Goods and Documentation.

- **Customer**
  - Excessive insistence of the customer to complete the transaction quickly.
  - Transactions which involve front or shell Companies.
  - Transactions which are between parties controlled by the same business entity.
  - Transactions which are inconsistent with the Customer's business and transaction history.
  - Transacting parties who share the same address or lack a valid address.
  - Clear disregard to apparent discrepancies by the Customer.

- **Country**
  - Inability of the Customer to produce invoices, bills of lading, or other appropriate documentation to support a requested Bank transaction.
  - A shipment to or from a jurisdiction designated as high risk for Money Laundering and Terrorist Financing activities (i.e. OFAC Sanctioned Countries).

- Trans-shipment of the trade goods through one or more jurisdictions for no apparent economic reason or any other justifiable reason.
- Receipt of cash or other payments from third party entities that have no apparent connection to the transaction

- **Goods**
- A significant discrepancy between the product/commodity's values as reported on the invoice and its fair market value.
- Trade goods that are designated as dual-use technologies or products.
- Trade goods that are designated as high-risk for money laundering and Terrorist Financing activities.
- An important discrepancy between the description of the trade goods on the invoice and the bill of lading/actual goods shipped.
- Unexpected changes to payment orders.
- Unusual use of intermediaries during the transaction process.

- **Documentation**
- Unnecessarily complex" and confusing transaction structures. These structures potentially aim to obscure a transaction's true purpose and nature.
- A payment method that does not match the risk characteristics of the transaction
- A transaction that involves the use of repeatedly amended or frequently extended terms (e.g. letters of credit)
- Requests by exporters to take back and replace trade and shipping documents, notably if the new documents provided have been altered or issued by a different entity
- Abnormal markings on monetary instruments.
- Modifications to third party documents, such as Customs Forms.

13.2 **Key findings about Trade Based Money Laundering**:

Trade-based Money Laundering is an important channel of criminal activity and given the growth in world trade; it represents increasingly important Money Laundering and Terrorist Financing vulnerability.

Trade-based Money Laundering practices vary in complexity. The most basic schemes are fraudulent trade practices (e.g. under- or over-invoicing of receipts). However, more complicated schemes integrate these fraudulent practices into a web of complex transactions which also involve the movement of value through the financial system (e.g. cheques or wire transfers) and/or the physical movement of banknotes (e.g. cash couriers). The use of these complex transactions further obscures the money trail and complicates detection.

Trade data analysis and the international sharing of trade data are useful tools for identifying trade anomalies, which may lead to the investigation and prosecution of trade-based money laundering cases.

While Law Enforcement Agencies (Customs, NFIU, Tax Authorities Banking Supervisors etc) can exchange trade-related information, this is restricted to certain circumstances undertaken on a voluntary rather than mandatory basis.

Identifying and combating trade-based Money Laundering is a bid difficult compared to other forms of money laundering and terrorist financing. This is in view of the limited understanding of the techniques of this form of money laundering by Financial Institutions and other Stakeholders. More training is required on Trade Based Money Laundering activities.

13.3 **Trade Based Money Laundering Red flags**:

The following are Money Laundering Red Flags:

- ✓ Significant discrepancies between the description of the commodity on the bill of lading and the invoice
- ✓ Significant discrepancies appear between the description of the goods on the bill of lading (invoice) and the actual goods shipped
- ✓ Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity fair market value.
- ✓ The size of the shipment appears inconsistent with the scale of the exporter or importer's regular business activities
- ✓ The type of commodity being shipped is designated as "high risk" for money laundering activities.
- ✓ The type of commodity being shipped appears inconsistent with the Exporter or Importer's regular business activities
- ✓ The shipment does not make economic sense
- ✓ The commodity is shipped to (or from) a jurisdiction designated as "high risk" for money laundering activities
- ✓ The commodity is trans-shipped through one or more jurisdictions for no apparent economic reason
- ✓ The method of payment appears inconsistent with the risk characteristics of the transaction
- ✓ The transaction involves the receipt of cash (or other payments) from third party entities that have no apparent connection with the transaction
- ✓ The transaction involves the use of repeatedly amended or frequently extended letters of credit.
- ✓ The transaction involves the use of front (or shell) companies.

13.4 **Measures to be taken when sign of Money Laundering is noticed**

- ✓ Run all transaction patterns against the red flags (mentioned above). Extra-precaution should be taken where similarities exists

- ✓ Conduct appropriate evaluation and Due Diligence (CDD) on Transactions and Products

- ✓ Run transactions through the Soft-Watch (Customer Identity Management System), available as a link on the Bank's Intranet Portal.

- ✓ Where match exists, discontinue the transaction and send a mail to regulatorycompliance@unitybankng.com or file a report addressed to the Chief Compliance Officer stating the Customer Name, Transaction Type, Customer Details, Transaction Amount and Remarks.

- ✓ Caution must be exercised to ensure that the Bank does not deal with customers whose origin or destination is listed among High Risk Countries and Non-Cooperative Countries and Territories (NCCTs / FATF Black list). Countries on the NCCT list include but are not limited to the following, and are subject to change from time to time.
    - Algeria
    - Afghanistan
    - Angola
    - Bosnia and Herzegovina
    - Democratic People's Republic of Korea (DPRK).
    - Guyana
    - Iran
    - Iraq
    - Lao People's Democratic Republic
    - Panama
    - Papua New Guinea
    - Syria
    - Uganda
    - Yemen
    - Ecuador
    - Indonesia
    - Myanmar.

- ✓ Examine cargo movements through the comparison of import / export documentation between two counties to verify that the data reported to one country's authorities matches the data reported to the other country's authorities.

- ✓ Examine domestic import data with an automated technique, such as Unit Price Analysis, to compare the average unit price for a particular commodity and identify traders who are importing commodities at a substantially higher or lower price than the world market.

- ✓ Using statistical analysis methods, such as linear regression models, on trade data concerning individual, non-aggregated imports and exports.

- ✓ Compare export information with tax declarations to detect discrepancies.
- ✓ Pay particular attention to trade transactions that display known red flag indicators of TB ML/FT/PF activity.
- ✓ Compare known typologies of risk (such as those identified in the FATF Typologies Report on Trade-based Money Laundering) with trade data information on cross-border monetary transfers associated with the payment of goods, intelligence, tax and wealth information.
- ✓ Take appropriate follow-up action when anomalies and discrepancies in trade and financial transactions are identified. Depending on the circumstances, appropriate follow-up action could involve asking the trader for further explanation and supporting documents; auditing traders who have presented discrepancies to check the volume of their business, regularity of their operations.
- ✓ File Suspicious Transaction / Activity Reports where there are reasonable grounds of suspicion on both activities / transactions

In order to forestall being used by Money Launderers and Terrorist Financiers Unity Bank Staff shall in processing Credit Facilities and processing Trade based transactions generally ensure proper due diligence on the customers that transact such businesses, beneficiaries of the proceeds as well as on the goods traded and the methods of transportation (i.e. vessels).

14.0 MONITORING OF UNUSUAL AND SUSPICIOUS TRANSACTIONS (MOT)

Continuous, up-to-date and regular monitoring of customer records and transactions is an essential ingredient of Unity Bank KYC policy. The extent of monitoring must be based on the risk sensitivity of the customer and account.

Staff shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

Transactions that involve large amount of cash inconsistent with the size of the balance maintained in the account and the customers' nature of business may indicate that the funds are being 'washed' through the account. High risk accounts should be subjected to intensive monitoring.

14.1 Methods of Transaction Monitoring

Unity Bank shall adopt a combination of the following methods:

- Traditional (Manual) Method

A pair of eyes: The first and most effective method of transaction monitoring is the vigilance by staff that processes the transactions, or interfaces with the customer/account. Its effectiveness is enhanced by training and experience

- Use of software solutions

The Bank has deployed a robust software for watching and monitoring activities on customer's transactions. The software has the capability to perform the following:

- **Threshold detection**: monitoring of transactions beyond a certain threshold.
- **Rules/Scenario detection**: Detecting a type of Money Laundering or Terrorism Financing behavior characterized by the occurrence of a rule or the occurrence of a high level behavior characterized by the co-occurrence of several rules.
- **Unusualness detection**: Monitoring of transactions that are inconsistent with expected behavior and/or exhibit affinity to aberrant/ anomalous behavior.

14.2 Scope of Transaction/Account Monitoring

The following types of transactions shall be monitored

- Transaction above prescribed threshold
- Monitor account for possible structuring
- Suspicious Transaction
- Transaction involving frequency that is unjustifiable or unreasonable
- Unusual or unjustified complex transactions
- Transaction having no apparent economic justification or lawful objective

All Staff are required to report any information which may come to their attention and which may give rise to knowledge or suspicion of Money Laundering and Terrorist Financing activities in the Bank.

14.3 Risk-Based Approach to Transaction Monitoring

Unity Bank shall seek to have:

- Adequate knowledge of customer transaction to know unusual/suspicious transactions
- Accounts classify into low, medium and high risk categories
- Intensify monitoring on high risk accounts.

Unity Bank shall monitor all transactions on a risk-sensitive basis using the following procedures:

- Determine the Bank's high-risk customers.
- Effect appropriate monitoring on these high - risk accounts
- Determine the type of account monitoring to be conducted. These may include: Real-time monitoring (payment filtering, thresholds etc)
- Retrospective monitoring (velocity of funds transfers, top high-risk customers and where they are transacting to high risk jurisdictions)
- Physical monitoring (Identification of suspicious transactions at time of occurring)

14.4 TERMINATING CUSTOMER RELATIONSHIPS

The Bank shall terminate business relationship with a customer where AML/CFT offence is established against the Customer. This is subject to:

- Approval of the Executive Compliance Officer.
- Communication of decision to terminate to the Customer

14.5 REPORTING REQUIREMENTS

The Bank shall ensure total adherence to the reporting regime of all the Regulatory Authorities as provided in the Money Laundering Provision Act 2011 (as amended), the Central Bank of Nigeria AML/CFT Regulation 2013:

- The Statutory return on Currency Transaction Report (CTR) Foreign Transaction Report (FTR) and Suspicious Transaction Report (STR) shall be rendered to the Nigerian Financial Intelligence Unit (NFIU) or other designated Agencies in the extensible Mark-up Language (XML) and EXCEL formats or in such other formats as may be prescribed from time to time.

- The XML Report Generator software shall be updated on periodic basis as soon as new schema is released by the Nigerian Financial Intelligence Unit (NFIU).

- Unity Bank shall conduct on-going monitoring of customer accounts and transactions on a risk sensitive basis. Unity Bank shall report all Suspicious and unusual transaction and shall cooperate fully with the Authorities.

- In addition to reporting suspected proceeds of crime and the Financing of Terrorism, these reports should also include suspicions related to activities involving Tax evasion and Bribery, where this is established. Designated Employees will co-operate with the Regulators/Law Enforcement Agencies to the extent obliged by law.

- Unity Bank would ensure at all times that adequate and effective analysis, processes and procedures are constantly in place to analyze all suspicious and unusual transactions or activity. In accordance with this Policy including any internal guidance issued in this regard, and subsequently reports such transactions to the NFIU.

- All Employees who have filed or intend to file a suspicious transaction/activity report should not discuss their suspicions with anyone other than their line Manager, Compliance Officers or the Chief Compliance Officer.

- The suspicion must under no circumstances be discussed with the customer as this would constitute tipping off. Tipping off is the disclosure of information to any person that is likely to prejudice an actual or potential investigation into ML/TF activities and is a

criminal offence. Also failure by Employee to report any suspicious transaction or activity relating to ML/TF is an offence.

- We shall ensure training is given to all categories of professional and non-professional staff of the bank. We shall also ensure continuous education of our Staff to facilitate the recognition and reporting of Money Laundering as required by Regulatory Bodies.

15.0 RECORD KEEPING / PRESERVATION

Money Laundering and Terrorist Financing Regulations requires Financial Institutions to maintain adequate records which are appropriate to the nature of the business and that can be used as evidence in any Investigation.

Records maintained should be such that:

- All legislation and KYC rules are met.
- Third parties i.e. External Auditors and Regulators can assess the effectiveness of the Bank 's observance of Money Laundering and Terrorist Financing procedures.
- All transaction effected by the Bank on behalf of any customer. All Customers can be properly identified and located.
- All Suspicious Reports both internal and external can be identified.
- The Bank can satisfy any enquiry from appropriate Authorities or Court orders.
- All files whether current or old are available in good time to meet any requests for documents.
- Files or documents either current or old will be held on the Bank 's premises and should be available within one working day of the request.
- Old items are stored off-site as set out in the Bank 's Archiving, Retrieval and Retention of Old Records Procedure. These items should be available within 3 working days of the request.
- Records relating to the evidence of identity must be kept for at least ten (10) years after the relationship with the Customer has ended. This would normally be from the date the Customer 's account was closed but in the case of a dormant account this can mean ten (10) years from the date of the last transaction on the account.
- Transaction records must also be kept for at least ten (10) years. The records should provide Investigating Authorities a satisfactory audit trail and establish a financial profile on any Suspect 's account.

- Records of Internal reports and disclosures to Regulators should be retained for at least ten (10) years. This may be lengthened if there is an investigation in progress requiring the Bank to further liaise with the Investigating Officer.

- The Bank must maintain records relating to Training and Compliance Monitoring. These must include formal records of the date of any Anti-Money Laundering Training, the nature of the Training and the names of the Members of Staff who received Training.

- Also maintained are reports submitted to the Chief Compliance Officer (CCO), correspondence concerning such reports and actions required and taken. This includes reports submitted to Management Committee and the Board.

- In line with relevant legislation, the Bank shall preserve and keep at the disposal of the Authorities, the records of Customers' identification as well as the Records of transactions including Suspicious Transactions report for a period of at least 10 years from the date of transactions or closure of the accounts or the severance of relationship with the customer.

- All documentary (files, folders etc), electronic (Compact Disks, Storage Media etc) records for both Account Opening, Transactional data and all other correspondences must be appropriately stored in Fire-Proof Cabinets in line with ISO provisions.

- All Information Systems used to prepare, generate and preserve all the afore-mentioned must be managed / preserved in line with ISO requirements (Unity Bank is ISO Compliant, having obtained ISO 27001 in 2013). It also has well entrenched ISMS policies for all its employees.

15.1 MAJOR ORGANISATIONS MANAGING AND SETTING STANDARDS ON AML/CFT

a. Financial Action Task Force (FATF)

- The Financial Action Task Force (FATF) is an inter-governmental body established in 1989 by the Ministers of its Member jurisdictions.

- The mandate of the FATF is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing of proliferation, and other related threats to the integrity of the international financial system.

- The Financial Action Task Force on Money Laundering is comprised of 36 member countries and territories and two international organizations1 and was organized to develop and promote policies to combat money laundering and terrorist financing.

- The FATF relies on a combination of annual self-assessments and periodic mutual evaluations that are completed by a team of FATF experts to provide information and to assess the compliance of its members to the FATF guidelines.

- FATF has no enforcement capability, but can suspend member countries that fail to comply on a timely basis with its guidelines. The FATF is housed at the headquarters of the Organization for Economic Cooperation and Development (OECD) in Paris and occasionally uses some OECD staff, but the FATF is not part of the OECD. The presidency of the FATF is a one-year appointed position,

- In collaboration with other international stakeholders, the FATF also works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.

- The FATF has developed a series of Recommendations that are recognised as the international standard for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. They form the basis for a coordinated response to these threats to the integrity of the financial system and help ensure a level playing field. First issued in 1990, the FATF Recommendations were revised in 1996, 2001, and 2003 and most recently in 2012 to ensure that they remain up to date and relevant, and they are intended to be of universal application.

- The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally.

b. ***FATF Mandate***

- When it was established in 1989, the FATF was charged with examining money laundering techniques and trends, reviewing the actions which had already been taken, and setting out the measures that still needed to be taken to combat money laundering.

- In 1990, the FATF issued a report containing a set of 40 recommendations,3 which provided a comprehensive plan of action to fight against money laundering. Following the terrorist attacks of September 11, 2001, the FATF redirected its efforts to focus on money laundering and terrorist financing.

- On October 31, 2001, the FATF issued a new set of guidelines and a set of eight special recommendations on terrorist financing. At that time, the FATF indicated that it had broadened its mission beyond money laundering to focus on combating terrorist financing and that it was encouraging all countries to abide by the new set of guidelines.

- A ninth (9th) special recommendation was added in 2005. In 2005, the United Nations Security Council adopted Resolution 1617 urging all U.N. Member States to implement the FATF 40 recommendations on money laundering and the nine special recommendations on terrorist financing.

- The FATF completed a review of its mandate and proposed changes that were adopted at the May 2004 ministerial meeting.

- In 2006, FATF adopted a new surveillance process, known as the International Cooperation Review Group, to identify, examine, and engage with vulnerable jurisdictions that are failing to implement effective AML-CFT (anti-money laundering/countering financing terrorism) systems.

- In addition, the FATF revised its mandate in 2008 to indicate that FATF "will intensify its surveillance of systemic criminal and terrorist financing risks to enhance its ability to identify, prioritize, and act on these threats." The FATF also expressed its support for the development of national threat assessments through best practice guidance and the establishment of stronger and more regular mechanisms for sharing information on risks and vulnerabilities

c. **Inter-Governmental Action Group against Money Laundering in West Africa (GIABA)**

- The establishment of the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) by the Authority of the ECOWAS Heads of State and Government in the year 2000 represents West Africa's response to the threats posed by transnational organized crime, particularly Money Laundering (ML) and Terrorist Financing (TF).

- The complex nature of Money Laundering (ML) and the numerous ways in which it manifests makes any accurate assessment of the harm it causes a complex task.

- GIABA uses tools and sources such as the Mutual Evaluation (ME) and Follow-up Reports (FPs), Typologies and other Research studies, Reports on Criminal Activities and investigations of ML/ TF cases in West African countries. It also uses the outcomes of technical needs assessments conducted to deliver Technical Assistance to GIABA member States. These bodies of information, when properly fused together, not only help to paint a picture of ML/TF in West Africa, but also inform better policy and operational decisions and actions.

d. ***Functions of GIABA***

- Ensure the adoption of measures against ML and TF in accordance with acceptable international standards and practices, including the FATF 40 Recommendations;

(a) Facilitate the adoption and implementation by member States of measures against ML/TF, taking into account specific regional peculiarities and conditions;
(b) Function as a forum where members can discuss matters of regional interest and share experiences;

(c) Organize self-evaluations and mutual evaluation exercises to determine the efficacy of measures adopted, including their conformity to acceptable international standards; and
(d) Co-ordinate and provide support to member States to establish and implement AML/CFT regimes including the implementation of laws against the proceeds of crime through Mutual Legal Assistance (MLA), and also, the establishment and maintenance of Financial Intelligence Units (FIUs).
(e) Whereas the FATF and some FSRBs were established as Task Forces, with fixed term but renewable mandate, GIABA was established by a Statute as a Specialized Institution of the ECOWAS

e. **Membership of GIABA*:***

Membership of GIABA consists of member States of the ECOWAS, namely;

(i) Republic of Benin
(ii) Burkina Faso
(iii) Republic of Côte d'Ivoire
(iv) Republic of Cape Verde
(v) Republic of The Gambia
(vi) Republic of Ghana
(vii) Republic of Guinea
(viii) Republic of Guinea Bissau
(ix) Republic of Liberia
(x) Republic of Mali
(xi) Republic of Niger
(xii) The Federal Republic of Nigeria
(xiii) Republic of Senegal
(xiv) Republic of Sierra Leone and
(xv) The Togolese Republic.

**Note: The Republic of Sao Tome and Principe is the only non-ECOWAS member of GIABA.

f. **Main Organs of GIABA**:

(i) The GIABA Ministerial Committee (GMC), consisting of the three Ministers responsible for Finance, Justice and Interior/Security of each member State;

(ii) The Secretariat, located in Dakar, Senegal;

(iii) The Technical Commission, consisting of experts drawn from the above-named ministries of member States; and

(iv) A network of National Correspondents, with one in each of the Member States. The functions of each organ are clearly stated in the GIABA Statutes.

g. **Nigerian Financial Intelligence Unit (NFIU)**

- The Nigerian Financial Intelligence Unit (NFIU) is the Central National Agency in Nigeria, responsible for the receipt and analysis of financial disclosure (Currency Transaction Reports and Suspicious Transaction Reports) and dissemination of intelligence generated there-from, to Competent Authorities for prosecution or otherwise.

- It was established in June 2004 to coordinate the Country's Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) regime.

- The NFIU is domiciled in the Economic & Financial Crimes Commission (EFCC),. The domiciliation of the NFIU within the EFCC (law enforcement agency) is strategic, given the peculiarities of the Nigerian economy and polity.

- The NFIU is a Member of the Egmont Group of Financial Intelligence Units. Since inception, it has worked in collaboration with the Intergovernmental Action Group against Money Laundering in West Africa (GIABA), to develop other FIUs within the sub-region, and to fully implement AML/CFT regime within the West African Sub-region. The NFIU also serves as the National Correspondence office for GIABA in Nigeria. In this capacity, the NFIU coordinates all activities of GIABA in the country.

The NFIU carries out other non-core functions, including

a) Monitoring Compliance with AML/CFT Requirements - to ensure compliance by reporting Entities.
b) Training and Research - to enhance the knowledge base of Stakeholders and aid AML/CFT policy formulation.

c) Enhance Public Awareness on AML/CFT Issues - through publicity in the print and electronic media, publication of newsletters etc.

d) Advisory Role- the NFIU provides inputs that help to fine-tune extant AML/CFT policies, regulations and laws based on findings from topology studies on Money Laundering/Terrorism Financing.

e) On a broader spectrum, the principal goal of the NFIU is to increase the transparency of Nigeria's financial and Designated Non-Financial systems so that Economic and Financial Crimes, particularly Money Laundering and Terrorist Financing, can be prevented or detected, investigated and successfully prosecuted.

Since its establishment, the NFIU has played significant role in deepening the implementation of AML/CFT regime in Nigeria, including:

- Providing a coordinated approach to the implementation of AML/CFT regime in Nigeria.

- Enhancing stakeholders' awareness and the compliance level of reporting institutions to AML/CFT requirements through capacity building etc.
- Facilitating the investigation and prosecution of Economic and Financial Crimes, through Intelligence to competent authorities.
- Facilitating the review/enactment of relevant AML / CFT Legal and Regulatory frameworks. For instance, the NFIU facilitated the presentation and consideration of the Anti-Terrorism bill by the National Assembly and the Review of MLPA 2004.
- Playing a leading role in delisting of Nigeria from the Financial Action Task Force (FATF) black list of Non Cooperating Countries and Territories, and the withdrawal of US Fin CEN Advisory - which hitherto affected foreign direct Investment and General Business transactions with Nigerian Banks.
- Supporting Government efforts in the provision of enabling environment for economic activities. The NFIU contributed significantly to the cleansing of the Financial and Designated Non-Financial Sectors, thereby improving Investors' confidence in the FIs and Designated Non-Financial Institutions (DNFIs) and enhancing their overall role in National Development.
- Played a key role in improving the image of Nigeria in the International Community.
- Contributed immensely in the delisting of Nigeria from the Non-Cooperative Countries & Territories list in June, 2006.

NFIU was moved from Observer to Full Membership Status in Egmont Group by first quarter 2007. It also contributed to the following:

a) Promoted enhanced quality of STRs submitted by reporting Entities
b) Implementation of online reporting system for STRs and CTRs
c) Achieved Increased awareness of FIU activities within Designated Non-Financial Institutions
d) Seamless exchange of Intelligence Information with FIUs worldwide
e) Contributed to Increased number of ML/TF Investigations and prosecutions through qualitative Intelligence.

15.2 TRAINING AND AML / CFT CULTURE AWARENESS

Unity Bank Training on AML/CFT shall encompass applicable AML/CFT laws and recent trends. The Training which is aimed at developing a culture of AML/CFT compliance among all Members of the Board, staff and stakeholders is to be conducted in phases.

All category of staff shall be trained on AML/CFT at least once in every financial year.

New entrants are equally given AML/CFT training during their induction course.

Specialised training shall be conducted for staff in specialized functions, including the ECO, CCO and all Compliance Officers.
The Bank shall put in place proper procedures, which generate a level of awareness and vigilance to guard against Money Laundering and Terrorist Financing.

Training of staff is very important in the bank's effort to fight Money Laundering and Terrorism Financing. Our Strategy is to focus more on front office Staff as they deal directly with the public and are first points of contact with potential Money Launderers.

Records of training will be kept, and all statutory returns on training will be rendered in line with relevant laws and regulations.

15.2.1 Training Attendance

Attendance is mandatory and any Bank's Staff that fails to turn up at the AML/ CFT training venue is to be sanctioned in line with existing Staff Policies.

15.3 VIRTUAL CURRENCY OPERATIONS.

Virtual currency or virtual money was defined in 2012 by the European Central Bank as "a type of unregulated, digital money, issued and usually controlled by its developers, used and accepted among the members of a specific virtual community.

Virtual or crypto currencies are largely untraceable and anonymous making them susceptible to abuse by criminals, especially in money laundering and financing of terrorism. In view of non-existent of adequate regulation on these activities, consumers may lose their money without any legal redress in the event these exchanges collapse or close business.

Examples of Virtual Currency includes Bitcoin, Ripples, Monero, Litecoin, Darkcoin, Peercoin, Primecoin, Dogecion, Onecoin etc.

Unity Bank does not allow use of virtual currencies within the network. Branches are therefore not allowed to use, hold, trade and/or transact in any way in virtual currencies;

All should note that Virtual Currency is Not a Legal Tender in Nigeria and should not be accepted as a payment medium for any Banking transaction.

15.4 UPDATE ON CBN ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (ADMINISTRATIVE) SANCTIONS REGULATIONS, 2018.

On April 25, 2018 the Central Bank of Nigeria issued via its website (Circular FPR/DIR/GEN/CIR/07/001 dated April 9, 2018) a new AML/CFT Administrative Sanctions Regulations 2018. The Regulation was developed in collaboration with the Office of the Attorney General of the Federation and was introduced to enable Nigeria comply with Financial Action Task Force (FATF) Recommendation 35 and the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) 2007 Mutual Evaluation recommendation. The recommendation requires Countries to have a range of effective, proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with natural or legal persons that fail to comply with AML/CFT requirements. The recommendation also states that "sanctions should be applicable not only to financial institutions but also to the Directors and Senior Management.

The new regime outlines administrative penalties (i.e. minimum monetary penalties) that could be imposed on:

- Financial Institution
- Members of the Board
- Managing Director/CEO
- Executive Compliance Officer
- Chief Risk Officer
- Chief Compliance Officer
- Internal Auditor

Imposition of Penalty	**Range of Penalty**
Bank	₦2 million to ₦20 million
Individuals	₦500,000 to ₦2.5 million

In determining its proposed course of action/penalty, the CBN will consider the following:

- Nature and seriousness of the infraction
- Conduct of the financial institution or the conduct of the person(s) concerned after the infraction;
- Previous record of the financial institution or the person(s) concerned; and
- Other general considerations such as:
    - ✓ the amount of any benefit gained or loss avoided due to the contravention;
    - ✓ how quickly the contravention was brought to the CBN's attention by the financial institution or person(s) concerned;

- ✓ whether the contravention was admitted or denied;
- ✓ likelihood of re-occurrence where no administrative sanction is imposed;
- ✓ remedial action taken when the contravention was identified (including any disciplinary action).

In addition to the above, where the Board, a director or officer responsible for ensuring compliance with the requirements has been penalized on 3 consecutive examination cycles and the breach continues, the CBN may suspend or remove the Board, Director, or officer of the institution. Unity Bank shall ensure full compliance with this Regulation

15.5 NIGERIAN FINANCIAL INTELLEGENCE UNIT (NFIU) ENFORCEMENT AND GUIDELINES

Nigerian Financial Intelligence Unit (NFIU) Enforcement and Guidelines to reduce Crime Vulnerabilities created by Cash withdrawal from Local Government Funds throughout Nigeria, Effective 1st June 2019. (NFIU/EXT/PRIV/ADV/DCEO/PRESIDENCY/23 AUG-2019/VOL.1/002)

The Bank shall adhere strictly with the following two requirements of the Guidelines as from 1st June, 2019:

- No withdrawal shall be made from State/Local Govt. Joint Government Account unless the withdrawal is to be credited into a particular Local Government Account.
- Cash withdrawal made from any Local Government Account anywhere in the Country should not exceed cumulative amount of N500,000.00 per day. Any other transactions after this threshold must be done through cheques or electronic funds transfer.

15.6 GENERAL DATA PROTECTION REGULATION (GDPR)/NIGERIA DATA PROTECTION REGULATION (NDPR) 2019

The General Data Protection Regulation (GDPR) and Nigeria Data Protection Regulation (NDPR) are legal frameworks that sets a road map on how data is collected, stored and transferred.

The NDPR which was released to the public on January 25, 2019 is aimed to protect Nigeria citizen's data and make sure such data are obtained for legitimate use.

The objectives of the Nigeria Data Protection Regulation (NDPR) 2019 issued by the National Information Technology Agency (NITDA) are as follow:

Safeguard the rights of natural persons to data privacy;
Foster safe conduct of transactions involving the exchange of personal data;
Prevent manipulation of personal data and
Ensure that Nigerian businesses remain competitive in international trade; through the safeguards afforded by a just and equitable legal regulatory framework on data protection and which regulatory framework is in tune with global best practices.

15.7 Compliance Obligations under NDPR, 2019 regulation.

- The Bank shall comply with the Nigeria Data Protection Regulation 2019 as follows:
- Formulation and communication of Data Privacy Protection Policy;
- Appointment of Data Protection Officer (DPO)
- Ensures that consent of a Data Subject has been obtained without fraud, coercion or undue influence;
- Inform the Data Subject of his right and the ease to withdraw his consent at any time;
- Inform the Data Subject where data may be transferred to a third party for any reason whatsoever; and obtain SGF approval where same is to be forwarded to a Foreign Country;
- Inform the Data Subject of the period for which the personal data will be stored;
- Conduct a detailed annual audit of its data privacy and data protection practices;
- Submit a summary of its data protection audit to the Agency (NITDA) on or before 15th March of the following year;
- Ensure the Bank is not found wanting by dealing with more than 10,000 Data Subjects to avoid a fine of 2% of Annual Gross Revenue of the preceding year or payment of the sum of 10 million naira whichever is greater etc.
- Annual certification of compliance with the Nigeria Data Protection Regulation (NDPR) 2019 requirements by a NITDA licensed Data Protection Compliance Organization (DPCOs).

16.0 COVID-19 PANDEMIC RISKS

Due to the Covid-19 Pandemic (corona virus) new trends emerged in the financial crimes landscape. This has led to financial system witnessing increase in fraudulent activities which necessitated the Financial Action Task Force (FATF), to release the following guidance:

- Criminals finding ways to bypass customer due diligence measures
- Increased misuse of online financial services and virtual assets to move and conceal illicit funds
- Exploiting economic stimulus measures and insolvency schemes as a means for natural and legal persons to conceal and launder illicit proceeds
- Increased use of the unregulated financial sector by creating additional opportunities for criminals to launder illicit funds
- Misuse and misappropriation of domestic and international financial aids and emergency funding
- Criminals and Terrorists exploiting COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries.

16.1 Identified COVID-19 Scams and Schemes

- Impersonation of officials in charge of controlling spread of the disease (impostors and scams)
- Counterfeiting, including of essential goods (such as medical supplies and medicines)
- Fundraising for fake Charities
- Fraudulent investment scams
- Cyber Crime
- Email and SMS phishing attacks
- Business email compromise scams

- Ransomware attacks (Virus attack from unknown sites)
- Human Trafficking and Exploitation of Workers
- Online Child Exploitation
- Organized Property Crime
- Increased remote transactions
- Unfamiliarity with online platforms
- Unregulated financial services
- Money Mules (Loan-Backed Money Laundering Schemes)

16.2 Mitigate to Identify COVID-19 Related Risks

In order to safe guard the Bank's assets and customers' funds from the COVID-19 related scams and other illicit activities. The bank shall continue to do the following:

- Continuous training of Compliance Officers, Internal Auditors, Resident Control Officers and Information Technology Risk Officers on the risks that could emanate from such incidence.
- Sensitize branches and all relevant stakeholders on the need to guard against such illicit and criminal activities.
- Continuous sensitization of Staff to minimize the fraudulent activities

16.3 PROCEDURE FOR ACCOUNT CLOSURE

Unity Bank shall take the following steps:

a) Receipt of Customer's instruction.
b) Date/Time stamp the instruction.
c) Verify customer's signature.
d) Inform Account Officer and Branch Service Manager of Customer's request.
e) Send Customer's letter requesting for closure to the relevant Branch Manager to indicate if there is an outstanding transaction.
f) The BM should interview the Customer to find out why the Customer wants to close the account and try to convince Customer to do otherwise.
g) If an account has a credit balance, advise Customer to issue a cheque for the balance less outstanding charges.
h) Refer account with debit balance to the Account Officer and/Branch Manager to ensure it is regularized before closure.
i) Retrieve signature card from the safe custody Cabinet and stamp "ACCOUNT CLOSED" on all the signature cards, sign and date the card.
j) Delete the scanned signature on the system.
k) In bold letters, write Account Closed on the front cover of the file.
l) Close the account on the system, and file away the closed account report generated on the system.

NOTE: Where a customer is closing an account for inability to provide or meet the Bank's KYC requirements, the account closure request should be escalated to Compliance for further action.

17.0 GLOSSARY AND DEFINATIONS OF TERMS

- **Competent Authorities**:

  All public Authorities with designated responsibilities for combating ML/TF offences

- **Designated Non-Financial Businesses and Professions (DNFBPs):**

  These are Non-Financial Businesses and Professions. ML/TF activities as relates to these Professionals are monitored by Special Control Unit on Money Laundering (SCUML).

- **Trust and Company Service Providers**:

  Acting as or arranging for another person to act as) a director, a trustee, a nominee or secretary of a company, a partner of the partnership, or a similar position in relation to other legal persons.

- **Payable through Accounts**:

  Correspondent Accounts that are used directly by third parties to transact businesses on their own behalf established or managed in an institutions name or for a third party institutions which customers may access independently to carry out their own transactions.

- **Shell Bank / Company**

  A Bank or Organization that has no physical presence in any jurisdiction and is not affiliated to a regulated Bank or subsidiary.

- **Money Laundering**:

  Any act or process that seeks to disguise the true origin, nature or ownership of the proceeds of a crime to appear legitimate. Money laundering offence occurs when an act or transaction takes place that involves the proceeds of crime.

- **Terrorist Financing:**

  Engaging in acts or transactions relating to financial, properties or other services or providing economic support where this is used to commit or facilitate the commission of a terrorist activity

- **Terrorist Activity:**

  Any act involving an element of violence or disruption, intended to threaten the national security or territorial integrity of a Country, intimidate the public or unduly compel Persons or Institutions to act in a particular manner with the aim of furthering a Political, Religious, Ideological or Philosophical motive.

- **Ultimate Beneficial Owner**:

  The natural person who ultimately owns or controls a customer and or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement.