Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) framework

Guaranty Trust Bank Limited ("the Bank"), is committed to the fight against all forms of financial crime, which includes, money laundering, terrorism financing, Proliferation financing, bribery and corruption, etc. To show this commitment, the Bank has continually implemented a framework for Anti-Money Laundering ("AML"), Combating the Financing of Terrorism ("CFT") and the Prevention of the Financing and Proliferation of Weapons of Mass Destruction. Strict adherence to this framework is mandatory for all employees.

The Bank's framework ensures compliance with AML/CFT legislation and regulations in Nigeria and has incorporated leading best practices including, but not limited to:

- The Financial Action Task Force (FATF) 40 Recommendations;
- Money Laundering (Prevention and Prohibition) Act 2022;
- Terrorism (Prevention and Prohibition) Act 2022:
- CBN AML/CFT Regulations 2013;
- Terrorism Prevention Regulations 2013;
- Corrupt Practices and Other Related Offences Act, Cap. C31, Laws of the Federation of Nigeria, 2004 ("the Act");
- UK Bribery Act 2010;
- USA Foreign Corrupt Practices Act;
- Proceeds of Crimes Act, 2022;
- Central Bank of Nigeria (CBN) Circulars.

Structure of the Framework

The Bank has developed policies and procedural guidelines and these documents are regularly reviewed/revised to ensure that they remain relevant and current and are in line with the evolving regulatory requirements and best practices. The policies and procedures clearly articulate the Bank's AML & CFT stance in the global fight against financial crime and are available on the Bank's intranet site for access to all employees at any point in time.

Annually, the Bank's Compliance Policies are reviewed and approved by the Board of Directors and where it is necessary to update the policy between cycles, an addendum is drafted for implementation and incorporated in the Policy at the next annual review.

The Bank has moved away from a "rule based, tick box" approach for combating financial crime risk to a risk-based approach. Consequently, the Bank identifies and assesses the risks from a proactive stance and allocates the requisite resources which center around systems and controls to manage these risks.

Scope of the Framework

The scope of the Bank's AML/CFT framework includes the following:

(i) Board and Management Responsibilities:

In accordance with AML/CFT global best practice, the "tone is set from the top". The Board of Directors of the Bank has oversight responsibilities for the AML/CFT framework. The Board ensures that the Bank's Management and all employees adhere strictly to all regulatory and internal procedures relating to AML/CFT and that the Bank maintains a zero-tolerance threshold to regulatory infraction. The Bank's Chief Compliance Officer is appointed by the Board of Directors and approved by the Central Bank of Nigeria (CBN).

(ii) Reports to Senior Management and the Board:

On a monthly and quarterly basis, AML/CFT reports are submitted to the Bank's Senior Management and the Board members respectively. These reports provide the Board and Senior Management with information to enable them to assess the Bank's compliance with its regulatory obligations. The reports also ensure that Directors and Senior Management are kept abreast on current trends and developments in the financial industry, particularly in the area of AML/CFT risk management.

(iii) Know Your Customer (KYC) Procedures:

To ensure that only customers that align with the Bank's risk appetite are on-boarded, duly completed account opening forms, identification document and other relevant information and documents are provided. This is the foundation/ bedrock for on boarding a customer in the Bank.

Customer Due Diligence (CDD) is conducted prior to entering any banking relationship with a customer. This includes at a minimum, identity and address verification as well as ascertaining the source of income and wealth of the customer.

Customers that are identified as high risk are subjected to Enhanced Due Diligence (EDD). EDD is conducted on such customers including Politically Exposed Persons (PEPs) to assess and manage the risks that the customers may pose. The approval of Senior Management and the Compliance team is required prior to the commencement of banking relationship with such high-risk customers

In compliance with regulatory requirements and perceived AML/CFT risk threats, Designated Non-Financial Businesses and Professionals (DNFBPs) and other similar businesses are required to undertake requisite and regulatory measures prior to account opening.

As part of the Bank's KYC and CDD procedures, identification documents are requested and obtained to confirm the ultimate beneficial owners of a business and the organization's control and structure.

Sanction screening is also conducted prior to entering a relationship as well as prior to effecting a transaction to ensure that the Bank does not enter a relationship with a sanctioned person/entity.

The Bank is also in compliance with the Foreign Account Tax Compliance Act (**FATCA**)and Common Reporting Standards criteria, and thus, have put measures in place to identify the defined persons in the Bank's database. All identified US persons are required to complete the requisite tax forms i.e., W8 BEN, W8 BEN-E and W9. A Customer who fails to complete the forms would be regarded as recalcitrant.

(iv) Transaction Monitoring:

Transaction monitoring is done using manual and automated methods. The former is performed by employees, who regularly identify red flags in transactions/activities and the latter resides within the Compliance team with the aid of transaction monitoring solutions.

Employees are aware that suspicious activities/ transactions should immediately be referred to the Compliance team.

Suspicious Transactions are brought to the attention of the Compliance team on a manual or automated basis; the former by way of employees filing internal suspicious transaction reports to the Compliance team and the latter by way of transaction monitoring tools reviewed by Compliance Officers. If deemed appropriate, reports are filed to the Nigerian Financial Intelligence Unit (NFIU).

To properly monitor transactions passing through the Bank's systems, the SAS AML tool, has been fully deployed in the Bank, providing an advancement in how transactions are monitored and investigated.

(v) Transaction Reporting:

Regulatory and statutory requirements stipulate that certain reports and returns are made to regulatory bodies. In Nigeria, the NFIU is the agency charged with the responsibility of receiving the following core transaction-based reports:

- Currency Transaction Report (CTR)
- Foreign Currency Transaction Report (FTR)
- Suspicious Transaction Report (STR)

The Bank renders reports to the **NFIU** and the CBN in accordance with the provisions of Sections 2, 3 and 7 of the Money Laundering (Prevention and Prohibition), Act 2022 ("the Act").

Section 2 of the Act provides that any lodgment or transfer of funds in excess of N5 million and above for individuals and N10 million and above for corporate customers must be reported.

Section 3 of the Act provides that financial institutions must submit a report on all international transfer of funds and securities of a sum exceeding ten thousand dollars ($10,000) or its equivalent in other foreign currencies.

Section 7 of the Act provides that a financial institution must submit a report on all unusual and suspicious transactions.

The Bank also, where applicable, in accordance with the Act, provides transaction-based reports to competent authorities as required

(vi) Relationship with Regulators and Law Enforcement Agencies:

The Bank maintains a cordial and supportive relationship with all regulatory and law enforcement agencies. The Bank promptly complies with and responds to all requests made, pursuant to the law, and provides information to regulators including the NFIU, the CBN and other relevant agencies.

The Bank is also at the forefront of cooperating with regulators to give feedback on new regulations and means to mitigate the risks that are being encountered in the financial industry brought on by new innovations and developing trends.

(vii) Sanctions Compliance Management:

As a policy, the Bank does not enter into any relationship with sanctioned individuals/entities. All employees, as applicable to their functions, are required to screen names of individuals and organizations who have or plan to enter a business relationship or carry out a transaction with/through the Bank against the Bank's internal watch list.

The internal watch list contains amongst others, the names of individuals and entities, who have been blacklisted by various regulatory bodies worldwide: Office of Foreign Asset Control (OFAC); European Union (EU); Her Majesty's Treasury (HMT); The Ministry of Economy, Finance and Industry in France (MINEFI); The United Nations (UN) and The Local List as provided by local regulatory and enforcement bodies.

Employees are required, as part of the Bank's policy, to refrain from any relationship and/or transaction which yield a true or positive match and follow the escalation procedure. Sanctions screening is done at account opening and on a real time basis for all SWIFT transactions.

(viii) Politically Exposed Persons (PEPs)

PEPs are individuals who are or have been entrusted with prominent public functions and the classification includes people or entities associated with them. Enhanced due diligence measures are applied to PEPs, as with other high-risk customers to mitigate

the AML/CFT risk they pose. This is to ensure that the Bank is not unknowingly supporting activities such as money laundering and/or the financing of terrorism.

In line with FATF's recommendation, the Bank employs the use of an automated monitoring tool in identifying and monitoring PEP transactions. This is achieved through the thorough review of information provided by customers and their transaction trends. Continuous monitoring is also carried out on these accounts.

On-boarding of new PEP accounts, as well as continuity of such accounts (for those already existing in the system) is subject to the approval of an Executive Director and the Compliance Team.

(ix) AML/CFT principles for Correspondent Banking:

The Bank only on-boards and maintains correspondent banking relationships with financial institutions that have implemented adequate AML/CFT policies and procedures. The Bank does not enter any form of relationships with shell banks nor maintain any payable through accounts. The Bank ensures that due diligence, including adverse media searches, are performed annually on our correspondent relationships to mitigate potential AML/CFT risks.

(x) Prohibited Business Relationships

In line with international best practice, the Bank does not open accounts or conduct transactions for customers using pseudonyms or numbers instead of actual names or maintain relationships with individuals or entities that have been sanctioned.

(xi) Risk Assessment

The Bank conducts Risk Assessment on its customers, products and services. This is to ensure that AML/CFT risks are identified, assessed and mitigated.

(xii) Anti-Bribery and Corruption (ABC) and Anti-Fraud)

The Bank upholds the highest standards of ethical conducts in all its activities and interactions. The Bank has zero tolerance for any form of bribery, corruption, fraud and unethical practices among employees, between the Bank and its employees, as well as between the Bank and external parties. The Bank also expects the same standards to be applied by third parties acting on behalf of the Bank. The Bank’s Board approved Ethics policy provides the requisite standards and principles on ethical conducts and practices expected and required of all staff and our related stakeholders.

(xiii) AML/CFT Training:

The Bank places a significant importance on the training of its employees. Training is conducted to ensure employees are well informed and up to date on the AML/CFT laws, KYC principles and the red flags of money laundering or terrorism financing which may occur in their job functions.

Annual Compliance training is mandatory for the Board members and all levels of staff, including Senior Management. Trainings are conducted via e-learning, face to face or on an ad hoc basis by email or via intranet slides to the appropriate personnel in relation to topical national and international findings. Tests are also conducted annually after the trainings to ensure that all employees have understood the training contents.

(xiv) AML/CFT Audits:

To ensure compliance with laws and regulations and to ensure an ever-evolving fit for use of the Compliance function, internal audit of the AML/CFT function is conducted on a quarterly basis. The purpose of the audit is to test the adequacy of the AML/CFT functions and ensure that the AML/CFT measures put in place by the Bank are up to date and effective.

The reports and findings of the audit are circulated to senior management. A follow-up to the audits takes place to ensure that the relevant issues are closed out and that the highlighted recommendations have been implemented. The Compliance function also undergoes a periodic independent audit by an external consultant in accordance with regulatory requirements.

(xv) Record Retention:

In accordance with regulations, customer identification documents are retained throughout the life of the account and for five (5) years after the cessation of the banking relationship. Transaction instruments are retained for five (5) years after the transaction date. In litigation and/or regulatory investigations, the records will be kept for as long as they are required.

(xvi) Data Protection:

The Bank has a duly approved Data Protection Policy which is revised on an ad-hoc basis to reflect the legal, regulatory and operating environment. The Bank adheres strictly to both local and international data protection policies such as the National Data Protection Regulations in countries where we operate and the European Union General Data Protection Regulation (**EU-GDPR**.)

(xvii) Whistle Blowing

The Bank has a Whistle Blowing Policy which is approved by the Board. This Policy governs the reporting and investigation of improper or Illegal activity at GTBank Limited, as well as the protection offered to the “Whistle blowers”.

All disclosures will be treated with strict confidence and the identity of the Whistle blower will not be revealed except where desired for Security, Regulatory or Legal purposes.

The following guidelines should be noted:

- Information provided should be disclosed in good faith backed by true and reasonable facts and /or evidence where possible;

- The Whistle blower/reporter should ensure that the disclosure is substantially true;
- Whistle blowing is not to be used for malicious acts or making false allegations;
- Whistle blowing is not to be used for personal vendetta or smear campaign;
- The Whistle blower shall be contacted by any of the recipients of the report where additional information is required.

GTBank's Whistle blowing method consist of a secure portal (hoisted on the intranet and internet) where the disclosure or whistleblowing information is logged.