Circle

AML and KYC Compliance Manual

TABLE OF CONTENT

INTRODUCTION

There have been increased stringent AML/CFT measures worldwide, particularly since the September 11, 2001 terrorist attacks in the U.S. Nigeria, not being left out in the global efforts to fight the menace, has taken some AML/CFT measures in recognition of the dangers posed.

With the enactment of AML legislations in Nigeria, the country is giving increased attention to implementing these laws. The AML and KYC Compliance Manual was developed for Circle's guidance under the regulatory purview of the CBN.

The Manual has been enriched by the enabling AML/CFT legislation enacted by Nigeria, particularly by the relevant FATF-Recommendations, the Guidelines of the Basle Committee on Banking Supervision and some international best practices documents.

PURPOSE AND OVERVIEW OF THE COMPLIANCE MANUAL

Money laundering (ML) has been defined as the process whereby criminals attempt to conceal the illegal origin and/or illegitimate ownership of property and assets that are the fruits or proceeds of their criminal activities. It is, thus, a derivative crime. Financing of Terrorism (FT) is defined here to include both legitimate and illegitimate money characterized by concealment of the origin or intended criminal use of the funds.

Money laundering and terrorist financing are global phenomena and there has been growing recognition in recent times, and indeed well-documented evidence, that both money laundering and terrorist financing pose major threats to international peace and security which could seriously undermine Nigeria's development and progress.

Consequently, concerted global efforts have been made to check these crimes. Financial institutions, in particular, have come under unprecedented regulatory pressure to enhance their monitoring and surveillance systems with a view to preventing, detecting and responding appropriately to money laundering and terrorist financing.

This Manual covers the following key areas of AML/CFT policy; compliance officer designation and duties; the need to cooperate with the competent/supervisory authorities; customer due diligence; monitoring and responding to suspicious transactions; reporting requirements; record keeping; AML/CFT employee training program, among others. Diligent implementation of the provisions of this Manual would not only minimize the risk of being used to launder the proceeds of crime but also provide protection against fraud and reputational and financial risks.

The Manual is structured in two parts. Part A is made up of the new AML/CFT Directives while Part B provides guidance on KYC.

1. PART A - AML/CFT DIRECTIVES

1.1 AML/CFT Institutional and Policy Framework

General Guidelines on Institutional Policy

Policies must be adopted to comply with AML/CFT obligations under the CBN regulatory directives, to actively prevent any transaction that otherwise facilitates criminal activity or terrorism.

Internal controls must be formulated and implemented, and other procedures that will deter criminals from using Circle's facilities for money laundering and terrorist financing.

AML/CFT Compliance Officer Designation and Duties

The AML/CFT Compliance Officer is designated with the relevant competence, authority and independence to implement Circle's AML/CFT compliance programme. The duties of the AML/CFT Compliance Officer, among others, include:

i. Developing an AML/CFT Compliance Programme;

ii. Receiving and vetting suspicious transaction reports from staff;

iii. Filing suspicious transaction reports with the CBN and NFIU ;

iv. Rendering "nil" reports with the CBN and NFIU, where necessary to ensure compliance;

v. Ensuring that Circle's compliance programme is implemented;

vi. Co-ordinating the training of staff in AML/CFT awareness, detection methods and reporting requirements; and

vii. Serving both as a liaison officer with the CBN and NFIU and a point-of-contact for all employees on issues relating to money laundering and terrorist financing.

Cooperation with Competent Authorities

Circle will comply promptly with all the requests made in pursuant with the law and provide information to the CBN, NFIU and other relevant government agencies.

The procedures for responding to authorized requests for information on money laundering and terrorist financing are required to meet the following:

i. searching immediately Circle's records to determine whether it maintains or has maintained any account for or has engaged in any transaction with each individual, entity, or organization named in the request;

ii. reporting promptly to the requesting authority the outcome of the search; and

iii. protecting the security and confidentiality of such requests.

Measures to Be Taken Against ML/TF

The company's secrecy and confidentiality laws shall not in no way, be used to inhibit the implementation of the requirements in this Manual. Relevant authorities are given the power required to access information to properly perform their functions in combating money l a u ndering and financing of terrorism; the sharing of information between competent authorities, either domestically or internationally; and the sharing of information between financial institutions, where this is required or necessary .

1.2 Customer Due Diligence (CDD)

Circle is not permitted to keep anonymous accounts or accounts in fictitious names.

When CDD is Required

Customer Due Diligence (CDD) measures will be carried out when:

i. business relations are established;

ii. carrying out occasional transactions above the applicable designated threshold of N250,000 or as may be determined by the CBN from time to time, including where the transaction is carried out in a single operation or several operations that appear to be linked; and

iii. carrying out occasional transactions that are wire transfers, including those applicable to cross-border and domestic transfers between financial institutions and when credit or debit cards are used as a payment system to effect money transfer. It does not, however, include the following types of payment: any transfer flowing from a transaction carried out using a credit or debit card so long as the credit or debit card number accompanying such transfers does flow from the transactions such as withdrawals from a bank account through an ATM machine, cash advances from a credit card or payment for goods; Circle -to- financial institution transfers and settlements where both the originator- person and the beneficial-person are acting on their own behalf.

iv. there is a suspicion of money laundering or terrorist financing, regardless of any exemptions or any other thresholds referred to in this Manual; or

v. there are doubts about the veracity or adequacy of previously obtained customer identification data.

Repeated identification and verification exercise is not required every time a customer conducts a transaction (after obtaining all the necessary documents and being so satisfied)

CDD Measures

1.2.1 Customers must be identified (whether permanent or occasional; natural or legal persons; or legal arrangements) using reliable, independently sourced documents, data or information. Full range of the CDD measures in this Manual must be carried out. However, in reasonable circumstances, the CDD measures can be applied on a risk-sensitive basis.

1.2.2 Types of customer information to be obtained and identification data to be used to verify the information are provided as Appendix A to this Manual.

In respect of customers that are legal persons or legal arrangements, the following is required:

i. verify any person purporting to have been authorized to act on behalf of such a customer by obtaining evidence of his/her identity and verifying the identity of such a person; and

ii. to verify the legal status of the legal person or legal arrangement by obtaining proof of incorporation from the Corporate Affairs Commission (CAC) or similar evidence of establishment or existence and any other relevant information.

1.2.3 The beneficial-owner must be identified and reasonable measures must be taken to verify his/her identity using relevant information or data obtained from a reliable source.

1.2.4 A customer acting on behalf of another person or not, must be determined. Where the customer is acting on behalf of another person, reasonable steps must be taken to obtain sufficient identification-data and to verify the identity of that other person.

1.2.5 Reasonable measures must be taken in respect of customers that are legal persons or legal arrangements to:

i. understand the ownership and control structure of such a customer; and

ii. determine the natural persons that ultimately own or control the customer.

The natural persons include those persons who exercise ultimate and effective control over the legal person or arrangement. Examples of types of measures needed to satisfactorily perform this function include:

For companies - The natural persons are those who own the controlling interests and those who comprise the mind and management of the company; and

For trusts – The natural persons are the settlor, the trustee and person exercising effective control over the trust and the beneficiaries.

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

1.2.6 Information on the purpose and intended nature of the business relationship of the potential customers must be obtained.

1.2.7 Ongoing due diligence must be conducted on the business relationship as stated by the customers above.

1.2.8 The ongoing due diligence above includes scrutinizing the transactions undertaken by the customer throughout the course of the relationship to ensure that the transactions being conducted are consistent with Circle's knowledge of the customer, its business and risk profiles, and the source of funds (where necessary).

1.2.9 Ensure that documents, data or information collected under the CDD-process are kept up-to -date and relevant by undertaking reviews of existing records, particularly the records in respect of higher-risk business-relationships or customer categories.

1.3 Higher Risk Categories of Customers

1.3.1 Enhanced due diligence must be performed for higher-risk categories of customer, business relationship or transaction. Examples of higher-risk customer categories include:

i. Non-resident customers;
ii. Private banking customers;
iii. Legal persons or legal arrangements such as trusts
iv. Companies that have nominee-shareholders or shares in bearer form; and
v. Politically exposed persons (PEPs), cross -border banking and business relationships, etc.

1.3.2 Where there are low risks, reduced or simplified measures can be applied. There are low risks in circumstances where the risk of money laundering or terrorist financing is lower, where 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. In circumstances of low-risk, simplified or reduced CDD measures can be applied when identifying and verifying the identity of these customers and the beneficial-owners.

1.4 Lower Risk Customers, Transactions or Products

1.4.1 These include:

i. Financial institutions – provided they are subject to requirements for the combat of money laundering and terrorist financing which are consistent with the provisions of this Manual and are supervised for compliance.

ii. Public companies (listed on a stock exchange or similar situations) that are subject to regulatory disclosure requirements;

iii. Government ministries and parastatals /enterprises;

iv. Life insurance policies where the annual premium and single monthly premium are within the threshold determined by NAICOM;

   a. Insurance policies for pension schemes if there is no surrender-value clause and the policy cannot be used as collateral;

   b. A pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme; and

v. Beneficial-owners of pooled-accounts held by Designated Non-Financial Businesses and Professions (DNFBPs) provided that they are subject to requirements to combat money laundering and terrorist financing consistent with the provisions of Money Laundering (Prohibition) Act.

1.4.2 Simplified or reduced CDD measures applied to customers resident abroad must be limited to customers in countries that have effectively implemented the FATF Recommendations.

1.4.3 Simplified CDD measures are not acceptable and therefore cannot apply to a customer whenever there is suspicion of money laundering or terrorist financing or specific higher risk scenarios. In such a circumstance, enhanced due diligence is mandatory.

1.4.4 CDD measures must be adopted on a risk sensitive-basis. Examples of higher risk categories are included in item 1.4.1(i – v) above and each case must be determined whether the risks are lower or not, having regard to the type of customer, product, transaction or the location of the customer. Where there is doubt, Circle is directed to clear with the CBN.

1.5 TIMING OF VERIFICATION

1.5.1 The identity of the customer, beneficial-owner and occasional customers must be verified before or during the course of establishing a business relationship or conducting transactions for them.

1.5.2 The verification of the identity of the customer and beneficial owner must be completed following the establishment of the business relationship, only when:

i. this can take place as soon as reasonably practicable;

ii. it is essential not to interrupt the normal business conduct of the customer; and

iii. the money laundering risks can be effectively managed.

1.5.3 Examples of situations where it may be essential not to interrupt the normal conduct of business are non face-to-face business.

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

1.6 EXISTING CUSTOMERS

1.6.1 **CDD requirements are applied to existing customers** on the basis of materiality and risk. Due diligence must be continually conducted on such existing relationships at appropriate times.

1.6.2 The appropriate time to conduct CDD is when (a) a transaction of significant value takes place, (b) customer documentation standards change substantially, (c) there is a material change in the way that the account is operated, and (d) there's apparent lack of sufficient information about an existing customer.

The customer must be properly identified in accordance with these criteria. The customer identification records should be made available to the AML/CFT compliance officer, other appropriate staff and competent authorities.

1.7 Definition of Politically Exposed Person (PEP)

1.7.1 Politically Exposed Persons (PEPs) are individuals who are or have been entrusted with prominent public functions both in foreign countries as well as in Nigeria. Examples of PEPs include, but are not limited to;

1.7.1.1 Heads of State or government;

1.7.1.2 Governors;

1.7.1.3 Local government chairmen;

1.7.1.4 Senior politicians;

1.7.1.5 Senior government officials;

1.7.1.6 Judicial or military officials ;

1.7.1.7 Senior executives of state owned corporations;

1.7.1.8 Important political party officials;

1.7.1.9 Family members or close associates of PEPs; and

1.7.1.10 Members of Royal Families.

1.7.2 In addition to performing CDD measures, appropriate risk management systems must be put in place to determine whether a potential customer or existing customer or the beneficial-owner is a politically exposed person.

1.7.3 Senior management approval must be obtained before a business relationship can be established with a PEP.

1.7.4 Where a customer has been accepted or has an ongoing relationship with Circle and the customer or beneficial-owner is subsequently found to be or becomes a PEP, senior management approval must be obtained in order to continue the business relationship.

1.7.5 Reasonable measures must be taken to establish the source of wealth and the sources of funds of customers and beneficial-owners identified as PEPs and report all anomalies immediately to the CBN and other relevant authorities.

1.7.6 Enhanced and ongoing monitoring must be conducted in the relationship In the event of any transaction that is abnormal, the account must be flagged and reported immediately to the CBN and other relevant authorities such as EFCC/NFIU .

1.8 Cross-Border Correspondent Banking

Correspondent banking is the provision of banking services by one bank (the correspondent bank) to another bank (the respondent bank). Large international banks typically act as correspondents for thousands of other banks around the world. Respondent banks may be provided with a wide range of services, including cash management (e.g. interest -bearing accounts in a variety of currencies), international wire transfers of funds, cheque clearing, payable -through-accounts and foreign exchange services.

1.8.1 In relation to cross-border and correspondent banking and other similar relationships. In addition to performing the normal CDD measures, the following measures must be taken:

- Gather sufficient information about a respondent institution to understand fully the nature of its business; and to determine from publicly available information the reputation of the institution and the quality of supervision, including whether or not it has been subject to a money laundering or terrorist financing investigation or regulatory action.
- Assess the respondent institution‘s AML/CFT - controls and ascertain that the latter are in compliance with FATF standards.
- Obtain approval from senior management before establishing correspondent relationships.
- Document the respective AML/CFT responsibilities of such institution.

1.8.2 Where a correspondent relationship involves the maintenance of payable - through-account, Circle should be satisfied that:

i. The customer (the respondent bank or Circle) has performed the normal CDD obligations on its customers that have direct access to the accounts of the correspondent financial institution; and

ii. the respondent financial institution is able to provide

1.8.3 Measures must be taken as may be needed to prevent the misuse of technological developments in money laundering or terrorist financing schemes such as internationally accepted Credit Cards .

1.8.4 Policies and procedures must be in place to address any specific risks associated with non-face to face business relationships or transactions . These policies and procedures shall be applied automatically when establishing customer relationships and conducting ongoing due diligence. Measures for managing the risks should include specific and effective CDD procedures that apply to non-face to face customers.

1.8.5 Necessary information should be obtained concerning property which has been laundered or which constitutes proceeds from, instrumentalities used in and intended for use in the commission of money laundering and financing of terrorism or other predicate offences. There must be confirmation that copies of identification data and other relevant documentation relating the CDD requirements will be made available from the third party upon request without delay.

i. There must be confirmation that the third party is a regulated and supervised institution and has measures in place to comply with requirements relevant customer identification data upon request to the correspondent financial institution.

1.9 New Technologies and Non-Face -To-Face Transactions

1.9.1 of CDD and reliance on intermediaries and other third parties on CDD as contained in this Manual.

1.10 Reliance on Intermediaries and Third Parties on CDD Function

1.10.1 If relying on intermediaries or other third parties which have no outsourcing or agency relationships, business relationships, accounts or transactions with Circle for their clients, some of the elements of the CDD process must be performed on the introduced business. The following criteria should also be met:

- Immediately obtain from the third party the necessary information concerning certain elements of the CDD process;
- Take adequate steps to certify that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;
- Satisfy themselves that the third party is regulated and supervised in accordance with Core Principles of AML/CFT and has measures in place to comply with the CDD requirements set out in this Manual; and
- Make sure that adequate KYC provisions are applied to the third party in order to get account information for competent authorities.

1.11 Maintenance of Records on Transactions

1.11.1 All necessary records of transactions must be maintained, both domestic and international, for at least five years following completion of the transaction (or longer if requested by the CBN and NFIU in specific cases). This requirement applies regardless of whether the account or business relationship is ongoing or has been terminated.

1.11.2 Examples of the necessary components of transaction-records include customer's and beneficiary's names, addresses (or other identifying information normally recorded by the intermediary), the nature and date of the transaction, the type and amount of currency involved, the type and identifying number of any account involved in the transaction.

1.11.3 Records of the identification data, account files and business correspondence must be maintained for at least five years following the termination of an account or business relationship (or longer if requested by the CBN and NFIU in specific cases).

1.11.4 Ensure that all customer-transaction records and information are available on a timely basis to the CBN and NFIU.

1.12 Attention on Complex and Unusual Large Transactions

1.12.1 Special attention must be paid to all complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose. Examples of such transactions or patterns of transactions include significant transactions relative to a relationship, transactions that exceed certain limits, very high account turnover inconsistent with the size of the balance or transactions which fall out of the regular pattern of the account's activity.

1.12.2 Background and purpose of such transactions must be examined as far back as possible and findings must be set forth in writing. Such findings must be reported to the CBN and NFIU; and kept available for the CBN, NFIU, other competent authorities and auditors for at least five years.

1.13 Suspicious Transactions and Compliance Monitoring

1.13.1 Definition of a Suspicious Transaction

There are numerous types of suspicious transactions and these reflect the various ways in which money launderers operate. For the purpose of this Manual, a suspicious transaction may be defined as one which is unusual because of its size, volume, type or pattern or otherwise suggestive of known money laundering methods. It includes such a transaction that is inconsistent with a customer's known, legitimate business or personal activities or normal business for that type of account or that lacks an obvious economic rationale.

1.13.2 Institutional Policy - There must be a written policy framework that would guide and enable Circle's staff to monitor, recognize and respond appropriately to suspicious transactions. A list of Money Laundering "Red Flags" is provided in Appendix C to this Manual.

1.13.3 An officer must be designated appropriately as the AML/CFT Compliance Officer to supervise the monitoring and reporting of suspicious transactions.

1.13.4 There must be alertness across board to the various patterns of conduct that have been known to be suggestive of money laundering and a checklist maintained of such transactions which should be disseminated to the relevant staff.

1.13.5 When any staff detects any "red flag" or suspicious money laundering activity, a "Review Panel" must be promptly instituted under the supervision of the AML/CFT Compliance Officer. Every action taken must be recorded. Staff are required to maintain confidentiality in respect of such investigation and any suspicious transaction report that may be 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).

1.13.6 Any suspicion that funds are the proceeds of a criminal activity or are related to terrorist financing, must be reported promptly to the CBN and NFIU. All suspicious transactions, including attempted transactions are to be reported regardless of the amount involved. This requirement applies regardless of whether the transactions involve tax matters or other things.

1.13.7 Circle's 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.

1.14 Internal Controls, Compliance and Audit

1.14.1 Internal procedures, policies and controls must be established and maintained to prevent money laundering and financing of terrorism and communicated to employees. These procedures, policies and controls should cover the CDD, record retention, the detection of unusual and suspicious transactions, the reporting obligation, among other things.

1.14.2 The AML/CFT compliance officer and appropriate staff are to have timely access to customer identification data, CDD information, transaction records and other relevant information.

1.14.3 Programs must be developed against money laundering and terrorist financing that include:

a) The development of internal policies, procedures and controls, including appropriate compliance management arrangement and adequate screening procedures to ensure high standards when hiring employees ;
b) An ongoing employee training programs to ensure that employees are kept informed of new developments, including information on current ML and CFT techniques, methods and trends; and that there is a clear explanation of all aspects of AML/CFT laws and obligations, and in particular, requirements concerning CDD and suspicious transaction reporting; and
c) Adequately resourced and independent audit function to test compliance with the procedures, policies and controls.

A structure must be put in place that ensures the operational independence of the Chief Compliance Officer (CCO).

1.15 Other Measures

These measures are meant to deter money laundering and terrorist financing. They include measures on sanctions, shell banks, other forms of reporting, special attention for higher risk countries and foreign branches and subsidiaries of Circle.

1.16 SANCTIONS

1.16.1 Any staff which fails to comply or contravenes the provisions contained in this Manual shall be subject to sanction. Any individual, being an official of Circle, who fails to take reasonable steps to ensure compliance with the provisions of this Manual shall be sanctioned accordingly. For purpose of emphasis, incidence of false declaration or false disclosure by the company's officers shall be subject to administrative review and sanction as stipulated in this Manual.

1.16.2 Any officer that contravenes the provisions of this Manual shall be subject to applicable sanctions as follows:

i. On the first infraction, be warned in writing
ii. On the second infraction, his /her appointment will be terminated and he/she be blacklisted from working in the financial services industry; and

1.16.3 In addition to the above regulatory sanctions, particulars of the individual(s) involved shall be forwarded to the relevant authorities such as EFCC, NPF, ICPC, etc for possible criminal investigation and prosecution.

1.17 ATTENTION FOR HIGHER RISK COUNTRIES

1.17.1 Special attention must be given to business relationships and transactions with persons (including legal persons and other financial institutions) from or in countries which do not or insufficiently apply the FATF recommendations.

1.17.2 Transactions that have no apparent economic or visible lawful purpose must be reported. The background and purpose of such transactions should, as far as possible, be examined and written findings made available to assist competent authorities such as CBN, NFIU, auditors and law enforcement agencies (LE As) to carry out their duties.

1.17.3 Business with foreign institutions which do not continue to apply or insufficiently apply the provisions of FATF Recommendations, the following measures must be taken:

i. Stringent requirements for identifying clients and enhancement of advisories, including jurisdiction-specific financial advisories for identification of the beneficial owners before business relationships are established with individuals or companies from that jurisdiction;
ii. Enhanced relevant reporting mechanisms or systematic reporting of financial transactions on the basis that financial transactions with such countries are more likely to be suspicious;

1.18 Foreign Branches and Subsidiaries

1.18.1 Ensure that foreign branches and subsidiaries observe AML/CFT measures consistent with the provisions of this Manual and to apply them to the extent that the local/host country's laws and regulations permit.

1.18.2 Ensure that the above principle is observed with respect to the branches and subsidiaries in countries which do not or insufficiently apply such requirements as contained in this Manual. Where these minimum AML/CFT requirements and those of the host country differ, branches and subsidiaries of Circle in the host country are required to apply the higher standard and such must be applied to the extent that the host country's laws, regulations or other measures permit.

1.18.3 Inform the CBN in writing when foreign branches or subsidiaries are unable to observe the appropriate AML/CFT measures because they are prohibited by the host country's laws, regulations or other measures.

1.18.4 Because Circle is subject to these AML/CFT principles, consistent application of the CDD measures at group levels is required, taking into account the activity of the customer with the various branches and subsidiaries.

1.19 AML/CFT Employee-education and Training Programme

1.19.1 **Institutional Policy -** Comprehensive employee education and training programs must be designed not only to make employees fully aware of their obligations but also to equip them with relevant skills required for the effective discharge of their AML/CFT tasks. Indeed, the establishment of such an employee training program is not only considered as best practice but also a statutory requirement.

1.19.2 A comprehensive training program is required to encompass staff/areas such as Compliance officers ; new staff (as part of the orientation program for those posted to the front office); operations/branch office staff (internal control/audit staff and managers.

1.19.3 The employee training program are required to be developed under the guidance of the AML/CFT Compliance Officer in collaboration with the top Management. The basic elements of the employee training program are expected to include:

i. AML regulations and offences
ii. The nature of money laundering
iii. Money laundering 'red flags' and suspicious transactions, including trade-based money laundering typologies
iv. Reporting requirements
v. Customer due diligence
vi. Risk-based approach to AML/CFT
vii. Record keeping and retention policy.

1.20 Monitoring Of Employee Conduct

1.20.1 Employees' accounts must be monitored for potential signs of money laundering and subject to the same AML/CFT procedures as applicable to other customers' accounts. This is required to be performed under the supervision of the AML/CFT Chief Compliance Officer. The latter's own account is to be reviewed by the Chief Internal Auditor or a person of adequate/similar seniority.

1.20.2 The AML/CFT performance review of staff is required to be part of employees' annual performance appraisals.

1.21 Protection Of Staff who Report Violations

1.21.1 Employees must always co-operate fully with the Regulators and law enforcement agents and to promptly report suspicious transactions to them.

1.21.2 Employees must make such reports confidential and will be protected from victimization for making them.

1.22 Additional Areas of AML/CFT Risks

1.22.1 Potential money laundering risks not covered by this Compliance Manual and report must be reviewed, identified and reported.

1.22.2 The AML/CFT frameworks must be reviewed from time to time with a view to determining its adequacy and identifying other areas of potential risks not covered.

2 PART B GUIDANCE ON KYC

A business relationship must not be established until all relevant parties to the relationship have been identified and the nature of the business to be conducted ascertained. Once an on-going business relationship is established, any inconsistent activity can then be examined to determine whether or not there is an element of money laundering for suspicion.

2.1 Duty to Obtain Identification Evidence

2.1.1 The first requirement of knowing your customer for money laundering purposes is to be satisfied that a prospective customer is who he/she is or claims to be.

2.1.2 Financial business or advisory to a customer or potential customer must not be provided unless it is certain who that person actually is. If the customer is acting on behalf of another, the identity of both the customer and the agent/trustee must be verified unless the customer is itself a Nigerian regulated financial institution.

2.1.3 Evidence must be obtained in respect of customers . There are certain exceptions to this duty as set out in this Manual. Since exemptions are difficult to apply, all relevant parties to the relationship must be identified from the outset. The general principles and means of obtaining satisfactory identification evidence are also set out below.

2.1.4 Nature and Level of the Business. Sufficient information must be obtained on the nature of the business that the customer intends to undertake, including the expected or predictable pattern of transactions.

2.1.5 The information collected at the outset for this purpose should include:

- purpose and reason for opening the account or establishing the relationship;
- nature of the activity that is to be undertaken;
- expected origin of the funds to be used during the relationship; and

- details of occupation/employment/business activities and sources of wealth or income.

2.1.6 Reasonable steps must be taken to keep the information up to date as the opportunities arise , such as when an existing customer opens a new account. Information obtained during any meeting, discussion or other communication with the customer are required to be recorded and kept in the customer's file to ensure, as far as practicable, that current customer information is readily accessible to the Money Laundering Compliance Officers (MLCO) or relevant regulatory bodies.

2.2 Apply Commercial Judgment

2.2.1 A risk-based approach must be taken at all times to 'Know Your Customer' requirements. The number of times to verify the customers' records must be decided during the relationship, the identification evidence required and when additional checks are necessary. These decisions are equally required to be recorded. For personal account relationships, all joint-account holders need to be verified. In respect of private company or partnership, focus should be on the principal owners/controllers and their identities must also be verified.

2.2.2 The identification evidence collected at the outset should be viewed against the inherent risks in the business or service.

2.3 Establishing Identity

2.3.1 Identification Evidence

The customer identification process should not start and end at the point of establishing the relationship but continue as far as the business relationship subsists.

The general principles for establishing the identity of both legal and natural persons and the guidance on obtaining satisfactory identification evidence set out in this Manual are by no meansexhaustive.

What is Identity?

2.3.2 Identity generally means a set of attributes such as names used, date of birth and the residential address at which the customer can be located. These are features which can uniquely identify a natural or legal person.

2.3.3 In the case of a natural person, the date of birth is required to be obtained as an important identifier in support of the name. It is, however, not mandatory to verify the date of birth provided by the customer.

2.3.4 Where an international passport/national identity card is taken as evidence of identity, the number, date and place/country of issue (as well as expiring date in the case of international passport) are required to be recorded.

When Must Identity be Verified?

2.3.5 Identity is required to be verified whenever a business relationship is to be established, on account opening or when series of linked transactions take place. **"Transaction" in this Manual is defined to include the giving of advice. The "**advice" here does not apply to when information is provided about the availability of products or services nor applies to when a first interview/discussion prior to establishing a relationship takes place.

2.3.6 Once identification procedures have been satisfactorily completed and the business relationship established, as long as contact or activity is maintained and records concerning that customer are complete and kept, no further evidence of identity is needed when another transaction or activity is subsequently undertaken.

Whose Identity Must Be Verified?

2.3.7 **(1) Clients** - sufficient evidence of the identity must be obtained to ascertain that the client is the very person he/she claims to be.

2.3.8 **(2) The person acting on behalf of another** - The obligation is to obtain sufficient evidence of identities of the two persons involved. This rule is however, subject to some exceptions. In consortium lending, the lead-manager/agent is required to supply a confirmation letter as evidence that he has obtained the required identity.

2.3.9 There is no obligation to look beyond the client where:

- the latter is acting on its own account (rather than for a specific client or group of clients);
- the client is a bank, broker, fund manager or other regulated financial institutions; and
- all the businesses are to be undertaken in the name of a regulated financial institution.

2.3.10 In other circumstances, unless the client is a regulated financial institution acting as agent on behalf of one or more underlying clients within Nigeria, and has given written assurance that it has obtained the recorded-evidence of identity to the required standards, identification evidence should be verified for:

i. **the named account holder/person** in whose name the funds is registered;

ii. **any principal beneficial owner of funds** who is not the account holder or named investor;

iii. **the principal controller(s) of an account** or business relationship (i.e. those who regularly provide instructions); and

iv. **any intermediate parties (e.g**. where an account is managed or owned by an intermediary).

2.3.11 Appropriate steps must be taken to identify directors and all the signatories to an account.

2.3.12 Joint applicants/account holders - identification evidence should be obtained for all the account holders.

2.3.13 For higher risk business undertaken for private companies (i.e. those not listed on the stock exchange) sufficient evidence of identity and address should be verified in respect of:

i. the principal underlying beneficial owner(s) of the company with 5% interest and above; and

ii. Those with principal control over the company's assets (e.g. principal controllers/directors).

2.3.14 Staff must be at alert to all circumstances that might indicate any significant changes in the nature of the business or its ownership and make enquiries accordingly and to observe the additional provisions for Higher Risk Categories of Customers under AML/CFT Directive in this Manual.

2.4 Timing of Identification Requirements

An acceptable time-span for obtaining satisfactory evidence of identity will be determined by the nature of the business, the geographical location of the parties and whether it is possible to obtain the evidence before commitments are entered into or money changes hands. However, any occasion when business is conducted before satisfactory evidence of identity has been obtained must be exceptional and can only be those circumstances justified with regard to the risk.

2.4.1 To this end, the following is required:

i. obtain identification evidence as soon as reasonably practicable after contact with the client with a view to agreeing with the client to carry out an initial transaction; or reaching an understanding (whether binding or not) with the client that future transactions may be carried out; and

ii. Where the client does not supply the required information as stipulated in (i) above , any activity with the client must be discontinued; and any understanding reached with the client must be brought to an end .

2.4.2 The application may however be processed immediately, provided that:

i. appropriate steps are promptly taken to obtain identification evidence; and

ii. No transfer or payment of any money is carried out to a third party until the identification requirements have been satisfied

2.4.3 An introduction from a respected customer, a person personally known to a Director or Manager or a member of staff often provides comfort but must not replace the need for identification evidence requirements to be complied with as set out in this Manual. Details of the person who initiated and authorized the introduction should be kept in the customer's mandate file along with other records. It is therefore mandatory that Directors/Senior Managers must insist on following the prescribed identification procedures for every applicant.

2.5 New Business for Existing Customers

2.5.1 When an existing customer closes one account and opens another or enters into a new agreement to purchase products or services, there is no need to verify the identity or address for such a customer unless the name or the address provided does not tally with the information in Circle's records. However, procedures are required to be put in place to guard against impersonation fraud. The opportunity of opening the new account should also be taken to ask the customer to confirm the relevant details and to provide any missing KYC information. This is particularly important:

- if there was an existing business relationship with the customer and identification evidence had not previously been obtained; or
- if there had been no recent contact or correspondence with the customer within the past three months; or
- when a previously dormant account is re -activated.

2.5.2 In the circumstances above, details of the previous account(s) and any identification evidence previously obtained or any introduction records should be linked to the new account-records and retained for the prescribed period in accordance with the provision of this Manual.

2.6 Recording Identification Evidence

2.6.1 Records of the supporting evidence and methods used to verify identity are required to be retained for a minimum period of five years after the account is closed or the business relationship ended.

2.6.2 Where the supporting evidence could not be copied at the time it was presented, the reference numbers and other relevant details of the identification evidence are required to be recorded to enable the documents to be obtained later. Confirmation is required to be provided that the original documents were seen by certifying on the record that the details were taken down as evidence.

2.6.3 Checks are made electronically and a record of the actual information obtained or of where it can be re-obtained must be retained as part of the identification evidence. Electronic records make the reproduction of actual information that would have been obtained before, less cumbersome.

2.7 Establishing Identity

Establishing identity under this Manual is divided into three broad categories:

- Private individual customers ;
- Quasi corporate customers ; and
- Pure corporate customers .

2.7.1 Private Individuals

2.7.1.1 General Information: The following information are to be established and independently validated for all private individuals whose identities need to be verified:

i. the true full name(s) used; and

ii. the permanent home address, including landmarks and postcode, where available.

The information obtained should provide satisfaction that a person of that name exists at the address given and that the applicant is that person. Where an applicant has recently moved from a house, the previous address should be validated.

2.7.1.2 **It is important to obtain the** date of birth as it is required by the law enforcement agencies. However, the information need not be verified. It is also important for the residence/nationality of a customer to be ascertained to assist risk assessment procedures.

2.7.1.3 A risk-based approach should be adopted when obtaining satisfactory evidence of identity. The extent and number of checks can vary depending on the perceived risk of the service or business sought and whether the application is made in person or through a remote medium such as telephone, post or the internet. However, for higher risk products, accounts or customers, additional steps should be taken to ascertain the source of wealth/funds.

2.7.2 Private Individuals Resident In Nigeria

The confirmation of name and address is to be established by reference to a number of sources. The checks should be undertaken by cross -validation that the applicant exists at the stated address either through the sighting of actual documentary evidence or by undertaking electronic checks of suitable databases, or by a combination of the two.

Physical Checks on Private Individuals Resident in Nigeria

2.7.2.1 It is mandatory to establish the true identities and addresses of customers and for effective checks to be carried out to protect the company against substitution of identities by applicants.

2.7.2.2 Additional confirmation of the customer's identity and the fact that the application was made by the person identified should be obtained through one or more of the following procedures:

i. internet sign-on following verification procedures where the customer uses security codes, tokens, and/or other passwords which had been set up during account opening and provided by mail (or secure delivery) to the named individual at an independently verified address;

ii. card or account activation procedures.

Additional information concerning the nature and level of the business to be conducted and the origin of the funds to be used within the relationship must be obtained from the customer.

2.7.3 Electronic Checks

2.7.3.1 A combination of electronic and documentary checks to confirm different sources of the same information provided by customers is required. The applicant's identity, address and other available information can be checked electronically by accessing data-bases or sources.

2.7.3.2 In respect of electronic checks, confidence as to the reliability of information supplied will be established by the cumulative nature of checking across a range of sources, preferably covering a period of time or through qualitative checks that assess the validity of the information supplied. The number or quality of checks to be undertaken will vary depending on the diversity as well as the breath and depth of information available from each source. Verification that the applicant is the data -subject also needs to be conducted within the checking process.

Some examples of suitable electronic sources of information are set out below:

i. An electronic search of the Electoral Register (is not to be used as a sole identity and address check);
ii. Access to internal or external account database ; and
iii. An electronic search of public records where available.

2.7.3.3 Application the above process and procedures will assist financial institutions to guard against impersonation, invented-identities and the use of false address. However, if the applicant is a non-face to face person, one or more additional measures must be undertaken for re-assurance.

2.8 "Financial Exclusion" For the socially but financially disadvantaged Applicants Resident In Nigeria

2.8.1 Access to basic banking facilities and other financial services is a necessary requirement for most adults. It is important therefore that the socially-but- financially disadvantaged should not be precluded from opening accounts or obtaining other financial services merely because they do not possess evidence

2.8.2 Where there are reasonable grounds to conclude that an individual client is not able to produce the detailed evidence of his identity and cannot reasonably be expected to do so, a letter or statement from a person in a position of responsibility such as solicitors, doctors, ministers of religion and teachers who know the client, confirming that the client is who he says he is, and confirming his permanent address, may be accepted as identification evidence.

2.8.3 When a client is treated as "financially excluded", it is required to record the reasons for treating the client as such.

2.8.4 The customer must be the person he/she claims to be. Therefore, where a letter/statement is accepted from a professional person, it should include a telephone number where the person can be contacted for verification. The information provided by the professional person must be verified from an independent source.

2.8.5 In order to guard against "financial exclusion" and to minimize the use of the exception procedure, an alternative documentary evidence of personal identity and address that can be accepted must be put in place.

2.8.6 Additional monitoring for accounts opened under the financial exclusion exception procedures must be conducted to ensure that such accounts are not misused.

2.9 Private Individuals not resident in Nigeria

2.9.1 For those prospective customers who are not resident in Nigeria but who make face -to- face contact, international passports or national identity cards should generally be available as evidence of the name of the customer. Reference numbers, date and country of issue should be obtained and the information recorded in the customer's file as part of the identification evidence.

2.9.2 A separate evidence of the applicant's permanent residential address must be obtained from the best available evidence, preferably from an official source. A "P.O. Box number" alone is not accepted as evidence of address. The applicant's residential address should be such that it can be physically located by way of a recorded description or other means.

2.9.3 Relevant evidence should be obtained directly from the customer or through a reputable credit or financial institution in the applicant's home country or country of residence. However, particular care must be taken when relying on identification evidence provided from other countries. The customer's true identity and current permanent address must be confirmed. **In such cases, copies of relevant identity documents should be sought and retained.**

2.9.4 Where a foreign national has recently arrived in Nigeria, reference might be made to his/her employer, university, evidence of traveling documents, etc. to verify the applicant's identity and residential address.

Private Individuals not Resident in Nigeria: Supply of Information

For a private individual not resident in Nigeria, who wishes to supply documentary information by post, telephone or electronic means, a risk - based approach must be taken. One separate item of evidence of identity must be obtained in respect of the name of the customer and one separate item for the address.

2.9.5 Documentary evidence of name and address can be obtained:

i. by way of original documentary evidence supplied by the customer; or
ii. by way of a certified copy of the customer's passport or national identity card and a separate certified document verifying address e.g. a driving licence, utility bill, etc; or
iii. through a branch, subsidiary, head office of a correspondent bank.

2.9.6 Where necessary, an additional comfort must be obtained by confirming the customer's true name, address and date of birth from a reputable credit institution in the customer's home country.

Use these requirements in conjunction with Appendix A to this Manual.

2.10 Non Face-to-Face Identification

2.10.1 Because of possible false identities and impersonations that can arise with non face-to-face customers, it is important to ensure that the applicant is who he/she claims to be. Accordingly, one additional measure or check should be undertaken to supplement the documentary or electronic evidence. These additional measures will apply whether the applicant is resident in Nigeria or elsewhere and must be particularly robust where the applicant is requiring an account with Circle.

2.10.2 Procedures to identify and authenticate the customer has to ensure that there is sufficient evidence either electronic or documentary to confirm his address and personal identity and to undertake at least one additional check to guard against impersonation fraud.

2.10.3 The extent of the identification evidence required will depend on the nature and characteristics of the product or service and the assessed risk. However, care must be taken to ensure that the same level of information is obtained for internet customers and other postal/telephone customers.

2.10.4 If reliance is being placed on intermediaries to undertake the processing of applications on the customer's behalf, checks should be undertaken to ensure that the intermediary are regulated for money laundering prevention and that the relevant identification procedures are applied. In all cases, evidence as to how identity has been verified should be obtained and retained with the account opening records.

2.10.5 Regular monitoring of internet-based business/clients must be conducted. If a significant proportion of the business is operated electronically, computerized monitoring systems /solutions that are designed to recognize unusual transactions and related patterns of transactions should be put in place to recognize suspicious transactions. AML/CFT compliance officers are required to review these solutions, record exemptions and report same quarterly to the CBN and NFIU.

2.11 Establishing Identity for Refugees and Asylum Seekers

2.11.1 A refugee and asylum seeker may require a Circle account without being able to provide evidence of identity. In such circumstances, authentic references from Ministry of Internal Affairs or an appropriate government agency should be used in conjunction with other readily available evidence.

2.11.2 Additional monitoring procedures should however be undertaken to ensure that the use of the account is consistent with the customer's circumstances.

2.12 Establishing Identity for Students and Minors

2.12.1 When opening accounts for students or other young people, the normal identification procedures set out in this Manual should be followed as far as possible. Where such procedures would not be relevant or do not provide satisfactory identification evidence, verification could be obtained:

- via the home address of the parent(s); or
- by obtaining confirmation of the applicant's address from his/her institution of learning; or
- by seeking evidence of a tenancy agreement or student accommodation contract.

2.12.2 Often, an account for a minor will be opened by a family member or guardian. In cases where the adult opening the account does not already have an account with Circle, the identification evidence for that adult, or of any other person who will operate the account should be obtained in addition to obtaining the birth certificate or passport of the child. It should be noted that this type of account could be open to abuse and therefore strict monitoring should then be undertaken.

2.12.3 For accounts opened through a school-related scheme, the school should be asked to provide the date of birth and permanent address of the student and to complete the standard account opening documentation on behalf of the student.

2.13 "Client Accounts" Opened By Professional Intermediaries

2.13.1 Stockbrokers, fund managers, solicitors, accountants, estate agents and other intermediaries frequently manage funds on behalf of their clients in "client accounts" opened with Circle. Such accounts may be general omnibus accounts holding the funds of many clients or they may be opened specifically for a single client. In each case, it is the professional intermediary who is Circle's customer. These situations should be distinguished from those where an intermediary introduces a client who himself becomes a customer.

2.13.2 Where the professional intermediary is itself covered and is indeed monitored by the money laundering regulations and AML/CFT supervisors respectively or their equivalent, identification can be waived on production of evidence .

2.13.3 However, where the professional intermediary is not regulated under the Money Laundering Regulations, the identity of the professional intermediary must not only be verified, but the identify of the person on whose behalf the professional intermediary is acting.

2.13.4 Where it is impossible to establish the identity of the person(s) for whom a solicitor or accountant is acting, a commercial decision based on the knowledge of the intermediary will be taken, as to the nature and extent of business that can be conducted. Reasonable enquiries about transactions passing through client- accounts that give cause for concern must be made.

2.14 Unincorporated Business/Partnerships

2.14.1 Where the applicant is an un-incorporated business or a partnership whose principal partners/controllers do not already have a business relationship with Circle, identification evidence should be obtained for the principal beneficial owners/controllers. This would also entail identifying one or more signatories in whom significant control has been vested by the principal beneficial owners/controllers.

2.14.2 Evidence of the trading address of the business or partnership should be obtained. A visit to the place of business might also be made to confirm the true nature of the business activities. For established businesses, a copy of the latest report and audited accounts can be obtained.

2.14.3 The nature of the business or partnership should be ascertained (but not necessarily verified from a partnership deed) to ensure that it has a legitimate purpose. In cases where a formal partnership arrangement exists, a mandate from the partnership authorizing the opening of an account or undertaking the transaction and conferring authority on those who will undertake transactions should be obtained.

2.15 Pure Corporate Customers

General Principles

2.15.1 Complex organizations and their structures, other corporate and legal entities are the most likely vehicles for money laundering. Those that are privately owned are being fronted by legitimate trading companies. Care should be taken to verify the legal existence of the applicant-company from official documents or sources and to ensure that persons purporting to act on its behalf are fully authorized. Enquiries should be made to confirm that the legal person is not merely a "brass-plate company" where the controlling principals cannot be identified.

2.15.2 The identity of a corporate company comprises:

i. registration number;
ii. registered corporate name and any trading names used;
iii. registered address and any separate principal trading addresses;
iv. directors;
v. owners and shareholders; and
vi. the nature of the company's business.

2.15.3 The extent of identification measures required to validate this information or the documentary evidence to be obtained depends on the nature of the business or service that the company requires. A risk-based approach should be taken. In all cases, information as to the nature of the normal business activities that the company expects to undertake should be obtained. Before a business relationship is established, measures should be taken by way of company search at the Corporate Affairs Commission (CAC) and other commercial enquiries undertaken to check that the applicant-company's legal existence has not been or is not in the process of being dissolved, struck off, wound up or terminated.

2.16 Non Face-to-Face Business

2.16.1 As with the requirements for private individuals, because of the additional risks with non face -to-face business, additional procedures must be undertaken to ensure that the applicant's business, company or society exists at the address provided and it is for a legitimate purpose.

2.16.2 Where the characteristics of the product or service permit, care should be taken to ensure that relevant evidence is obtained to confirm that any individual representing the company has the necessary authority to do so.

2.16.3 Where the principal owners, controllers or signatories need to be identified within the relationship, the relevant requirements for the identification of personal customers should be followed.

2.17 Low Risk Corporate Business

Public Registered Companies

2.17.1 Corporate customers that are listed on the stock exchange are considered to be publicly owned and generally accountable. Consequently, there is no need to verify the identity of the individual shareholders.

2.17.2 Similarly, it is not necessary to identify the directors of a quoted company. However, there must be appropriate arrangements to ensure that the individual officer or employee (past or present) is not using the name of the company or its relationship with Circle for a criminal purpose. The Board Resolution or other authority for any representative to act on behalf of the company in its dealings with Circle should be obtained to confirm that the individual has the authority to act. Phone calls can be made to the Chief Executive Officer of such a company to intimate him of the application to open the account.

2.17.3 No further steps should be taken to verify identity over and above the usual commercial checks where the applicant company is:

i. listed on the stock exchange; or

ii. there is independent evidence to show that it is a wholly owned subsidiary or a subsidiary under the control of such a company.

2.17.4 Due diligence will normally be conducted where the account or service required falls within the category of higher risk business.

2.18 Private Companies

2.18.1 Where the applicant is an unquoted company and none of the principal directors or shareholders already have an account with Circle, the following documents should be obtained from an official or recognized independent source to verify the business itself:

i. a copy of the certificate of incorporation/registration, evidence of the company's registered address and the list of shareholders and directors;

ii. a search at the Corporate Affairs Commission (CAC) or an enquiry via a business information service to obtain the information in (i) above; and

iii. an undertaking from a firm of lawyers or accountants confirming the documents submitted to the CAC.

2.18.2 Attention should be paid to the place of origin of the documents and the background against which they were produced. If comparable documents cannot be obtained, then verification of principal beneficial owners/controllers should be undertaken.

2.19 Higher Risk Business

Bank Accounts for Registered Public Companies

2.19.1 Where a higher-risk business applicant is seeking to enter into a full relationship or any other business relationship where third party funding and transactions are permitted, the following evidence must be obtained either in documentary or electronic form:

i. For established companies (those incorporated for 18 months or more) a set of the latest report and audited accounts is required to be produced;

ii. A search report at the CAC or an enquiry via a business information service or an undertaking from a firm of lawyers or accountants confirming the documents submitted to the CAC;

- A certified copy of the resolution of the Board of Directors to open an account and confer authority on those who will operate it; and
- The Memorandum and Article of Association of the company.

2.20 Higher Risk Business Relating to Private Companies

2.20.1 For private companies undertaking higher risk business (in addition to verifying the legal existence of the business**)** the principal requirement is to look behind the corporate entity to identify those who have ultimate control over the business and the company's assets . What constitutes significant shareholding or control for this purpose will depend on the nature of the company. Identification evidence is required to be obtained for those shareholders with interests of 5% or more.

The principal control rests with those who are mandated to manage the funds, accounts or investments without requiring authorization and who would be in a position to override internal procedures and control mechanisms.

2.20.2 Identification evidence should be obtained for the principal-beneficial owner(s) of the company and any other person with principal control over the company's assets. Where the principal owner is another corporate entity, the objective is to undertake measures that look behind that company or vehicle and verify the identity of the beneficial-owner(s) or settlors. When it is apparent that the principal- beneficial owners/controllers have changed, they are required to ensure that the identities of the new ones are verified.

2.20.3 The directors who are not principal controllers and signatories to an account must be identified for risk based approach purpose.

2.20.4 In respect of a full relationship (irrespective of whether or not the turnover is significant) a visit to the place of business must be undertaken to confirm the existence of business premises and the nature of the business activities conducted.

2.20.5 If suspicions are aroused by a change in the nature of the business transacted or the profile of payments through a bank or investment account, further checks should be made to ascertain the reason for the changes .

2.20.6 For full relationships, periodic enquiries are required to be made to establish whether there have been any changes to controllers, shareholders or to the original nature of the business or activity.

2.20.7 Particular care should be taken to ensure that full identification and "Know Your Customer" requirements are met if the company is an International Business Company (IBC) registered in an offshore jurisdiction and operating out of a different jurisdiction.

2.21 Foreign Financial Institutions

2.21.1 For foreign financial institutions, the confirmation of existence and regulated status should be checked by one of the following means:

i. checking with the home country's Central Bank or relevant supervisory body; or
ii. checking with another office, subsidiary, branch, or correspondent bank in the same country; or
iii. checking with Nigerian regulated correspondent bank of the overseas institution; or
iv. obtaining evidence of its license or authorization to conduct financial and banking business from the institution itself .

2.21.2 Additional information on banks all over the world can be obtained from various international publications and directories or any of the international business information services.

References made to these publications are not meant to replace the confirmation evidence required above.

2.22 Other Institutions Clubs and Societies

2.22.1 In the case of applications made on behalf of clubs or societies, reasonable steps must be taken to ensure the legitimate purpose of the organization by sighting its constitution. The identity of at least two of the principal contact persons or signatories should be verified initially in line with the requirements for private individuals. The signing authorities should be structured to ensure that at least two of the signatories that authorize any transaction has been verified. When signatories change, the identity of at least two of the current signatories must be verified.

2.22.2 Where all the members would be regarded as individual clients, all the members in such cases are required to be identified in line with the requirements for personal customers. Each situation should be looked at on a case-by-case basis.

Charities in Nigeria

2.22.3 Adherence to the identification procedures required for money laundering prevention purpose would remove the opportunities for opening unauthorized accounts with false identities on behalf of charities. Confirmation of the authority to act in the name of the charity is clearly mandatory.

2.22.4 The practice of opening unauthorized accounts of this type under sole control is strongly discouraged. For emphasis, accounts for Charities in Nigeria are required to be operated by a minimum of two signatories, duly verified and documentation evidence obtained.

Registered Charities

2.22.5 When dealing with an application from a registered charity, the name and address of the charity concerned must be obtained and confirmed.

2.22.6 To guard against the laundering of fraudulently obtained funds (where the person making the application or undertaking the transaction is not the official correspondent or the recorded alternate), a letter must be sent to the official correspondent, informing him of the Charity's application before it. The official correspondent should be requested to respond as a matter of urgency especially where there is any reason to suggest that the application has been made without authority.

2.22.7 Where a charity is opening an account, the identity of all signatories should be verified initially and when the signatories change, care should be taken to ensure that the identity of any new signatory is verified.

2.22.8 Applications on behalf of un-registered charities should be dealt with in accordance with procedures for clubs and societies set out in item 2.22.1 of this Manual.

Religious Organizations (ROs)

2.22.9 A religious organization is expected by law to be registered by 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 at least two signatories to its account must be verified.

Three - Tiers of Government/Parastatals

2.22.10 Where the applicant for business is any of the above, the legal standing of the applicant, including its principal ownership and the address must be verified. A certified copy of the Resolution or other documents authorizing the opening of the account or to undertake the transaction should be obtained in addition to evidence that the official representing the body has the relevant authority to act.

2.22.11 Telephone contacts must also be made with the Chief Executive Officer of the organization/parastatals concerned, intimating him of the application to open the account in Circle.

Foreign Consulates

2.22.12 The authenticity of applicants that request to open accounts or undertake transactions in the name of Nigerian-resident foreign consulates and any documents of authorization presented in support of the application should be checked with the Ministry of Foreign Affairs or the relevant authorities in the Consulate's home country.

2.23 Intermediaries of Other Third Parties to Verify Identity to Introduce Business Who to rely upon and the circumstances

2.23.1 It is reasonable , in a number of circumstances, for reliance of information verification to be placed on another financial institution to:

i. undertake the identification procedure when introducing a customer and to obtain any additional KYC information from the client; or

ii. confirm the identification details if the customer is not resident in Nigeria; or

iii. confirm that the verification of identity has been carried out (if an agent is acting for underlying principals).

Introductions from Authorized Financial Intermediaries

2.23.2 Where an intermediary introduces a customer and then withdraws from the ensuing relationship altogether, then the underlying customer has become the applicant for the business. He must, therefore, be identified in line with the requirements for personal, corporate or business customers as appropriate. An introduction letter should therefore be issued by the introducing financial institution or person in respect of each applicant for business. To ensure that product-providers meet their obligations, that satisfactory identification evidence has been obtained and will be retained for the necessary statutory period, each introduction letter must either be accompanied by certified copies of the identification evidence that has been obtained in line with the usual practice of certification of identification documents or by sufficient details/reference numbers, etc that will permit the actual evidence obtained to be re-obtained at a later stage.

Written Applications

2.23.3 For a written application (unless other arrangements have been agreed that the service provider will verify the identity itself) a financial intermediary must provide along with each application, the customer's introduction letter together with certified copies of the evidence of identity which should be placed in the customer's file.

2.23.4 If these procedures are followed, the product provider, stockbroker or investment banker will be considered to have fulfilled its own identification obligations. However, if the letter is not forthcoming from the intermediary, or the letter indicates that the intermediary has not verified the identity of the applicant, the service provider is required to satisfy its obligation by applying its own direct identification procedures.

Non-Written Application

2.23.5 Product providers receiving non-written applications from financial intermediaries (where a deal is placed over the telephone or by other electronic means) have an obligation to verify the identity of customers and ensure that the intermediary provides specific confirmation that identity has been verified. A record must be made of the answers given by the intermediary and retained for a minimum period of five years. These answers constitute sufficient evidence of identity in the hands of the service provider.

Introductions from Foreign Intermediaries

2.23.6 Where introduced business is received from a regulated financial intermediary who is outside Nigeria, the reliance that can be placed on that intermediary to undertake the verification of identity-check must be assessed by the MLCO or some other competent persons within Circle on a case by case basis based on the knowledge of the intermediary.

Corporate Group Introductions

2.23.7 Where a customer is introduced by one part of a financial sector group to another, it is not necessary for identity to be re-verified or for the records to be duplicated provided that:

i. the identity of the customer has been verified by the introducing parent company, branch, subsidiary or associate in line with the money laundering requirements to equivalent standards and taking account of any specific requirements such as separate address verification;

ii. no exemptions or concessions have been applied in the original verification procedures that would not be available to the new relationship;

iii. a group introduction letter is obtained and placed with the customer's account opening records; and

iv. in respect of group introducers from outside Nigeria, arrangements should be put in place to ensure that identity is verified in accordance with requirements and that the underlying records of identity in respect of introduced customers are retained for the necessary period.

2.23.8 Where there is day-to-day access to all the Group's "Know Your Customer" information and records , there is no need to identify an introduced customer or obtain a group introduction letter if the identity of that customer has been verified previously. However, if the identity of the customer has not previously been verified, then any missing identification evidence will need to be obtained and a risk-based approach taken on the extent of KYC information that is available on whether or not additional information should be obtained.

2.23.9 It must be ensured that there is no secrecy or data protection legislation that would restrict free access to the records on request or by law enforcement agencies under court order or relevant mutual assistance procedures. If it is found that such restrictions apply, copies of the underlying records of identity should, wherever possible, be sought and retained.

2.23.10 Where identification records are held outside Nigeria, the records available must be ascertained to have, in fact, met the requirements in this Manual.

2.24 Business Conducted by Agents

2.24.1 Where an applicant is dealing in its own name as agent for its own client, the identity of the underlying client must be verified.

Evidence is sufficient if it is established that the client:

i. is bound by and has observed this Manual or the provisions of the Money Laundering (Prohibition) Act, 2004; and

ii. is acting on behalf of another person and has given a written assurance that he has obtained and recorded evidence of the identity of the person on whose behalf he is acting.

2.24.2 Where such an assurance cannot be obtained, then the business should not be undertaken.

2.24.3 In circumstances where an agent is either unregulated or is not covered by the relevant money laundering legislation, then each case should be treated on its own merits. The knowledge of the agent will inform the type of the due diligence standards to apply. Risk-based approach must also be observed.

Syndicated Lending

2.24.4 For syndicated lending arrangements, the verification of identity and any additional KYC requirements rest with the lead-manager or agent required to supply the normal confirmation letters.

Correspondent Relationship

2.24.5 Transactions conducted through correspondent relationships need to be managed, taking a risk-based approach. "Know Your Correspondent" procedures are required to be established to ascertain whether or not the correspondent bank or the counter- party is itself regulated for money laundering prevention. If regulated, the correspondent is required to verify the identity of its customers in accordance with FATF- standards. Where this is not the case, additional due diligence will be required to ascertain and assess the correspondent's internal policy on money laundering prevention and know your customer procedures.

2.24.6 The volume and nature of transactions flowing through correspondent accounts with financial institutions from high risk jurisdictions or those with inadequacies or material deficiencies should be monitored against expected levels and destinations and any material variances should be checked.

2.24.7 Records of having ensured that sufficient due diligence has been undertaken by the remitting bank on the underlying client and the origin of the funds in respect of the funds passed through their accounts , should be exhaustively maintained.

2.24.8 Establishing correspondent relationships with high risk foreign banks (e.g. shell banks with no physical presence in any country) should be guarded against.

2.24.9 Staff dealing with correspondent banking accounts are required to be trained to recognize higher risk circumstances and be prepared to challenge the correspondents over irregular activity (whether isolated transactions or trends) and to submit a suspicious activity report to the CBN and NFIU.

2.24.10 Accounts should be terminated with correspondent banks that fail to provide satisfactory answers to reasonable questions including confirming the identity of customers involved in unusual or suspicious circumstances.

2.25 Acquisition Of a Financial Institution

2.25.1 When a financial institution is acquired, it is not necessary for the identity of all the existing customers to be re-identified, provided that all the underlying customers' records are acquired with the business. It is, however, important to carry out due diligence enquiries to confirm that the acquired institution had conformed with the requirements in this Manual.

2.25.2 Verification of identity should be undertaken as soon as it is practicable for all the transferred customers who were not verified by the transferor in line with the requirements for existing customers that open new accounts, where:

i. the money laundering procedures previously undertaken have not been in accordance with the requirements of this Manual;
ii. the procedures cannot be checked; or
iii. where the customer-records are not available

2.26 Multiple Family Applications

Where multiple family applications are received and the aggregate subscription price is US $1,000 or more; and N250,000 or more for an individual person, then identification evidence will not be required for:

i. a spouse or any other person whose surname and address are the same as those of the applicant
ii. a joint account holder; or
iii. an application in the name of a child where the registration in the names of minors is prohibited. The account is to be registered with the name of the family member of full age who signed the application form.

2.27 Linked Transactions

2.27.1 If it appears to a person handling applications that a number of single applications under $1,000 and N500,000 in different names are linked (e.g. payments from the same Circle account) apart from the multiple family applications above, identification evidence must be obtained in respect of parties involved in each single transaction.

2.27.2 Installment payment issues should be treated as linked transactions where it is known that total payments will amount to $1,000 or its equivalent or N250,000 for an individual; or N500,0000 for body corporate or such other monetary amounts as may, from time to time, be stipulated by any applicable money laundering legislation or guidelines. Either at the outset or when a particular point has been reached, identification evidence must be obtained.

2.27.3 Applications that are believed to be linked and money laundering is suspected are required to be processed on a separate batch for investigation after allotment and registration has been completed. Returns with the documentary evidence are to be rendered to the CBN and NFIU accordingly. Copies of the supporting cheques, application forms and any repayment-cheques must be retained to provide an audit trail until the receiving financial institution is informed by CBN, NFIU or the investigating officer that the records are of no further interest.

2.28 Sanctions for Non-Compliance with KYC

Failure to comply with the provisions contained in this Manual will attract appropriate sanction in accordance with existing laws and as detailed in the AML/CFT section of this Manual.

APPENDIX A:

INFORMATION TO ESTABLISH IDENTITY

A. Natural Persons

For natural persons the following information should be obtained, where applicable:

- Legal name and any other names used (such as maiden name);
- Correct permanent address (full address should be obtained and a Post Office box number is not sufficient);
- Telephone number, fax number, and e-mail address;
- Date and place of birth;
- Nationality;
- Occupation, public position held and name of employer;
- An official personal identification number or other unique identifier contained in an unexpired official document such as passport, identification card, residence permit, social security records or driving license that bears a photograph of the customer;
- Type of account and nature of the banking relationship; and
- Signature.

This information should be verified by at least one of the following methods:

- Confirming the date of birth from an official document (e.g. birth certificate, passport, identity card, social security records);
- Confirming the permanent address (e.g. utility bill, tax assessment, bank statement, a letter from a public authority);
- Contacting the customer by telephone, by letter or by e-mail to confirm the information supplied after an account has been opened (e.g. a disconnected phone, returned mail, or incorrect e-mail address should warrant further investigation);
- Confirming the validity of the official documentation provided through certification by an authorized person (e.g. embassy official, notary public).

The examples quoted above are not the only possibilities. There may be other documents of an equivalent nature which may be produced as satisfactory evidence of customers' identity.
Equally effective customer identification procedures must be applied for non-face -to-face customers as for those available for interview.

From the information provided, an initial assessment of a customer's risk profile should be made. Particular attention needs to be focused on those customers identified as having a higher risk profile . Additional inquiries made or information obtained in respect of those customers should include the following:

- Evidence of an individual's permanent address sought through a credit reference agency search, or through independent verification by home visits;
- Personal reference (i.e. by an existing customer);
- Prior bank reference and contact with the bank regarding the customer;
- Source of wealth;
- Verification of employment, public position held (where appropriate).

The customer acceptance policy should not be so restrictive to amount to a denial of access by the general public to banking services, especially for people who are financially or socially disadvantaged (see details in AML/CFT Compliance Manual).

B. Institutions

The term institution includes any entity that is not a natural person. In considering the customer identification guidance for the different types of institutions, particular attention should be given to the different levels of risk involved.

i. Corporate Entities

For corporate entities (i.e. corporations and partnerships), the following information should be obtained:

- Name of institution;
- Principal place of institution's business operations;
- Mailing address of institution;
- Contact telephone and fax numbers;

- Some form of official identification number, if available (e.g. Tax identification number);
- The original or certified copy of the Certificate of Incorporation and Memorandum and Articles of Association;
- The resolution of the Board of Directors to open an account and identification of those who have authority to operate the account;
- Nature and purpose of business and its legitimacy.

This information should be verified by at least one of the following methods:

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

Reasonable steps should be taken to verify the identity and reputation of any agent that opens an account on behalf of a corporate customer, if that agent is not an officer of the corporate customer.

ii) Corporations/Partnerships

For corporations/partnerships, the principal guidance is to look behind the institution to identify those who have control over the business and the company's/partnership's assets, including those who have ultimate control.

For corporations, particular attention should be paid to shareholders, signatories, or others who inject a significant proportion of the capital or financial support or otherwise

exercise control. Where the owner is another corporate entity or trust, the objective is to undertake reasonable measures to look behind that company or entity and to verify the identity of the principals.

What constitutes control for this purpose will depend on the nature of a company, and may rest in those who are mandated to manage the funds, accounts or investments without requiring further authorization, and who would be in a position to override internal procedures and control mechanisms.

For partnerships, each partner should be identified and it is also important to identify immediate family members that have ownership control.

Where a company is listed on a recognized stock exchange or is a subsidiary of such a company then the company itself may be considered to be the principal to be identified. However, consideration should be given to whether there is effective control of a listed company by an individual, small group of individuals or another corporate entity or trust. If this is the case then those controllers should also be considered to be principals and identified accordingly.

C. Other Types of Institution

The following information should be obtained in addition to that required to verify the identity of the principals in respect of Mutuals/Friendly Societies, Cooperatives and Provident Societies, Charities, Clubs and Associations, and Professional Intermediaries:

- Name of account;
- Mailing address;
- Contact telephone and fax numbers;
- Some form of official identification number, such as tax identification number;
- Description of the purpose/activities of the account holder as stated in a formal constitution; and
- Copy of documentation confirming the legal existence of the account holder such as the register of charities.

This information should be verified by at least one of the following:

- Obtaining an independent undertaking from a reputable and known firm of lawyers or accountants confirming the documents submitted;
- Obtaining prior bank references; and
- Accessing public and private databases or official sources.

(i) Mutual/Friendly, Cooperative and Provident Societies

Where these entities are an applicant for an account, the principals to be identified should be considered to be those persons exercising control or significant influence over the organization's assets. This often includes board members, executives and account signatories.

(ii) Charities, Clubs and Associations

In the case of accounts to be opened for charities, clubs, and societies, reasonable steps should be taken to identify and verify at least two signatories along with the institution itself. The principals who should be identified should be considered to be those persons exercising control or significant influence over the organization’s assets. This includes members of the governing body or committee, the President, board members, the treasurer, and all signatories.

In all cases, independent verification should be obtained that the persons involved are true representatives of the institution. Independent confirmation should also be obtained of the purpose of the institution.

(iii) Professional Intermediaries

When a professional intermediary opens a client account on behalf of a single client that client must be identified. Professional intermediaries will often open "pooled" accounts on behalf of a number of entities. Where funds held by the intermediary are not co - mingled but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary should be identified. Where the funds are co-mingled, the beneficial-owners should be looked through. However, there may be instances where it becomes unnecessary to look beyond the intermediary (e.g. when the intermediary is subject to the same due diligence standards in respect of its client base as Circle).

APPENDIX B

DEFINITION OF TERMS

For the proper understanding of this Manual, certain terms used within are defined as follows:

Terms	Definition
Applicant for Business	The person or company seeking to establish a 'business relationship' or an occasional customer undertaking a 'one-off' transaction whose identity must be verified.
Beneficial owner	Beneficial owner refers to the natural person(s) who ultimately owns or controls a customer and/or the person on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
Business Relationship	'Business relationship' is any arrangement between Circle and the applicant for business whose purpose is to facilitate the carrying out of transactions between the parties on a 'frequent, habitual or regular' basis and where the monetary value of dealings in the course of the arrangement is not known or capable of being ascertained at the outset.
Cross-borde r transfer	Cross-border transfer means any wire transfer where the originator and beneficiary institutions are located in different jurisdictions. This term also refers to any chain of wire transfers that has at least one cross-border element.

Designated categories of offences	Designated categories of offences means: ● participation in an organized criminal group and racketeering; ● terrorism, including terrorist financing; ● trafficking in human beings and migrant smuggling; ● sexual exploitation, including sexual exploitation of children; ● illicit trafficking in narcotic drugs and psychotropic substances; ● illicit arms trafficking; ● illicit trafficking in stolen and other goods; ● corruption and bribery; ● fraud; ● counterfeiting currency; ● counterfeiting and piracy of products; ● environmental crime; ● murder, grievous bodily injury; ● kidnapping, illegal restraint and hostage-taking; ● robbery or theft; ● smuggling; ● extortion; ● forgery; ● piracy; and ● insider trading and market manipulation.
Designated non-financial businesses and professions	Designated non-financial businesses and professions means: a) Casinos (which also includes internet casinos). b) Real estate agents. c) Dealers in precious metals. d) Dealers in precious stones. Lawyers, notaries, other independent legal professionals and accountants – this refers to sole practitioners, partners or employed professionals within professional firms. It is not meant to refer to "internal" professionals that are employees of other types of businesses, nor to professionals working for government agencies, who may already be subject to measures that would combat money laundering. e) Company Service Providers refers to all persons or businesses that are not covered elsewhere under these Recommendations, and which as a business, provide any of the following services to third parties: i. acting as a formation agent of legal persons; ii. acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons; iii. providing a registered office; business address or

	iv. accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement; v. acting as (or arranging for another person to act as) a trustee of an express trust; vi. acting as (or arranging for another person to act as) a nominee shareholder for another person.
Domestic transfer	Domestic transfer means any wire transfer where the originator and beneficiary institutions are both located in Nigeria . This term therefore refers to any chain of wire transfers that takes place entirely within Nigeria's borders, even though the system used to effect the wire transfer may be located in another jurisdiction.
False declaration *False disclosure*	False declaration refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the declaration or otherwise requested by the authorities. This includes failing to make a declaration as required. False disclosure refers to a misrepresentation of the value of currency or bearer negotiable instruments being transported, or a misrepresentation of other relevant data which is asked for in the disclosure or otherwise requested by the authorities. This includes failing to make a disclosure as required
The FATF Recommendations	The FATF Recommendations refers to the Forty Recommendations and to the Nine Special Recommendations on Terrorist Financing.
Financial institutions	Financial institutions means any person or entity who conducts as a business one or more of the following activities or operations for or on behalf of a customer: 1. Acceptance of deposits and other repayable funds from the public. 2. Lending. 3. Financial leasing. 4. The transfer of money or value. 5. Issuing and managing means of payment (e.g. credit and debit cards, cheques, traveller's cheques, money orders and bankers' drafts, electronic money). 6. Financial guarantees and commitments. 7. Trading in: (a) money market instruments (cheques, bills, CDs, derivatives etc.); (b) foreign exchange; (c) exchange, interest rate and index instruments;

	(d) transferable securities; (e) commodity futures trading. 8. Participation in securities issues and the provision of financial services related to such issues. Individual and collective portfolio management. 10. Safekeeping and administration of cash or liquid securities on behalf of other persons. 11. Otherwise investing, administering or managing funds or money on behalf of other persons. 12. Underwriting and placement of life insurance and other investment related insurance. 13. Money and currency changing. The list is not exhaustive but subject to the definition contained in BOFIA 1991 (as amended).
Legal arrangements	Legal arrangement refers to express trusts or other similar legal arrangements.
Legal persons	Legal persons refer to bodies corporate, foundations, partnerships, or associations, or any similar bodies that can establish a permanent customer relationship with Circle.
Non-profit Organizations/Non-governmental Organizations	The term non-profit organization/non governmental organizations refers to a legal entity or organization that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of ? good works.

Payable through account	Payable through account refers to correspondent accounts that are used directly by third parties to transact business on their own behalf.
Proceeds	Proceeds refers to any property derived from or obtained, directly or indirectly, through the commission of an offence.
Property	Property means assets of every kind, whether corporeal or incorporeal, moveable or immoveable, tangible or intangible, and legal documents or instruments evidencing title to, or interest in such assets.
Risk	All references to risk in this Manual refer to the risk of money laundering and/or terrorist financing.
Settlor	Settlors are persons or companies who transfer ownership of their assets to trustees
Shell bank	Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial services group that is subject to effective consolidated supervision. Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.
Terrorist	It refers to any natural person who: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and willfully; (ii) participates as an accomplice in terrorist acts; (iii) organizes or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Terrorist act	A terrorist act includes but are not limited to: (i) An act which constitutes an offence within the scope of, and as defined in one of the following treaties: Convention for the Suppression of Unlawful Seizure of Aircraft (1970), Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971), Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents

	(1973), International Convention against the Taking of Hostages (1979), Convention on the Physical Protection of Nuclear Material (1980), Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1988), Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (1988), Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms located on the ContinentalShelf (1988), and the International Convention for the Suppression of Terrorist Bombings (1997); and (ii) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from doing any act.
Terrorist financing	Terrorist financing (FT) includes the financing of terrorist acts, and of terrorists and terrorist organizations.
Terrorist financing offence	A terrorist financing (FT) offence refer not only to the primary offence or offences, but also to ancillary offences.
Terrorist organization	Refers to any group of terrorists that: (i) commits, or attempts to commit, terrorist acts by any means, directly or indirectly, unlawfully and wilfully; (ii) participates as an accomplice in terrorist acts; (iii) organizes or directs others to commit terrorist acts; or (iv) contributes to the commission of terrorist acts by a group of persons acting with a common purpose where the contribution is made intentionally and with the aim of furthering the terrorist act or with the knowledge of the intention of the group to commit a terrorist act.
Those who finance Terrorism	Those who finance terrorism refers to any person, group, undertaking or other entity that provides or collects, by any means, directly or indirectly, funds or other assets that may be used, in full or in part, to facilitate the commsision of terrorist acts, or to any persons or entities acting on behalf of, or at the direction of such persons, groups, undertakings or other entities. This includes those who provide or collect funds or other assets with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist acts.

Trustee	Trustees, include paid professionals or companies or unpaid persons who hold the assets in a trust fund separate from their own assets.
Unique identifier	A unique identifier refers to any unique combination of letters, numbers or symbols that refer to a specific originator.

APPENDIX C:

MONEY LAUNDERING AND TERRORIST FINANCING "RED FLAGS"

1. INTRODUCTION

Monitoring and reporting of suspicious transactions is key to AML/CFT effectiveness and compliance. Effective and efficient transaction monitoring programmes must be put in place to facilitate the process.

Although the types of transactions which could be used for money laundering are numerous, it is possible to identify certain basic features which tend to give reasonable cause for suspicion of money laundering.

This appendix, which lists various transactions and activities that indicate potential money laundering, is not exhaustive. It does reflect the ways in which money launderers have been known to operate.

Transactions or activities highlighted in this list are not necessarily indicative of actual money laundering if they are consistent with a customer's legitimate business. Identification of any of the types of transactions listed here should provoke further investigation to determine their true legal status.

2. SUSPICIOUS TRANSACTIONS "RED FLAGS"

(i) Potential Transactions Perceived or Identified as Suspicious

- Transactions involving high-risk countries vulnerable to money laundering, subject to this being confirmed.
- Transactions involving shell companies.
- Transactions with correspondents that have been identified as higher risk.
- Large transaction activity involving monetary instruments such as traveller's cheques, bank drafts, money order, particularly those that are serially numbered.

- Transaction activity involving amounts that are just below the stipulated reporting threshold or enquiries that appear to test Circle's own internal monitoring threshold or controls.

(ii) Lending Activity

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

(iii) Terrorist Financing "Red flags"

- Persons involved in currency transaction share an address or phone number, particularly when the address is also a business location or does not seem to correspond to the stated occupation (e.g., student, unemployed, or self - employed).
- Financial transaction by a nonprofit or charitable organisation, for which there appears to be no logical economic purpose or for which there appears to be no link between the stated activity of the organisation and other parties in the transaction.

- Large number of incoming or outgoing funds transfers takes place through a business account, and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves designated high- risk locations.

- The stated occupation of the customer is inconsistent with the type and level of account activity.

- Funds transfer does not include information on the originator, or the person on whose behalf the transaction is conducted, the inclusion of which should ordinarily be expected.

- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.

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

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

(iv) Other Unusual or Suspicious Activities

- Employee exhibits a lavish lifestyle that cannot be justified by his/her salary.
- Employee fails to comply with approved operating guidelines, particularly in private banking.
- Employee is reluctant to take a vacation.
- Customer uses a personal account for business purposes.
- Official Embassy business is conducted through personal accounts.
- Embassy accounts are funded through substantial currency transactions.
- Embassy accounts directly fund personal expenses of foreign nationals.