

FRAMEWORK FOR AML/CFT RBS REGULATION FOR FINANCIAL INSTITUTIONS (FI)

CONTENTS

A. INTRODUCTION

| | |
|--|-----------|
| 1. BACKGROUND ----- | 1 |
| 2. SUSPICIOUS TRANSACTION REPORT----- | 1 |
| 3. MLPA & CBN AML/CFT REGULATION----- | 2 |
| 4. MONEY LAUNDERING AND TERRORIST FINANCING----- | 3 |
| 5. OVERVIEW OF ML/FT RISK ASSESSMENT----- | 4 |
| Customers and entities ----- | 4 |
| Geographic locations----- | 5 |
| Analysis of specific risk categories ----- | 5 |
| Developing financial institution’s AML/CFT compliance program based upon Risk assessment----- | 6 |
| Consolidated AML/CFT compliance risk assessment----- | 6 |
| Updating of risk assessment by financial institution----- | 7 |
| Minimum requirements of AML/CFT compliance----- | 7 |
| Internal controls----- | 7 |
| Independent testing----- | 9 |
| Chief compliance officer ----- | 11 |
| Training ----- | 12 |

| | |
|--|-----------|
| 6. OVERVIEW OF PROCEDURES FOR REGULATORY REQUIREMENTS AND RELATED TOPICS ----- | 13 |
| . OVERVIEW OF CUSTOMER IDENTIFICATION PROGRAM ----- | 13 |
| Verification through documents----- | 13 |
| Verification through non-documentary methods----- | 14 |
| Record-keeping and retention requirements----- | 14 |
| Comparison with terrorist lists----- | 14 |
| Adequate customer notice----- | 15 |
| 7. IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT----- | 15 |
| Reliance on another financial institution ----- | 15 |
| Use of third parties----- | 16 |
| Other legal requirements----- | 16 |
| Inquiries and requests by PEPs----- | 16 |
| Funds transfer records----- | 16 |
| Monetary Instruments records----- | 17 |
| Surveillance Monitoring (Automated Account Monitoring) ----- | 17 |
| STR completion and filing ----- | 17 |
| 8. OVERVIEW OF CURRENCY TRANSACTION REPORTING----- | 17 |
| Aggregation of currency transactions----- | 18 |
| Filing time frames and record retention requirements----- | 18 |
| CTR back-filing----- | 18 |
| Information sharing between law enforcement and financial institutions----- | 18 |
| Search requirements----- | 18 |
| Restrictions and confidentiality----- | 19 |
| Documentation----- | 20 |
| Voluntary information sharing----- | 21 |
| Notice to share information given to CBN/NFIU----- | 21 |

| | |
|--|-----------|
| 9. OVERVIEW OF PURCHASE AND SALE OF MONETARY INSTRUMENTS RECORD-KEEPING- | 22 |
| Purchaser verification----- | 22 |
| Indirect currency purchases of monetary instruments----- | 22 |
| Record keeping and retention requirements----- | 23 |
| 10. OVERVIEW OF FUNDS TRANSFERS RECORD-KEEPING----- | 24 |
| Responsibilities of originator’s financial institutions record-keeping requirements-- | 24 |
| Additional record-keeping requirements for non-established customers----- | 25 |
| Payment orders made in person----- | 25 |
| Payment orders not made in person----- | 25 |
| Irretrievability----- | 26 |
| Travel rule requirement----- | 26 |
| Responsibilities of intermediary institutions----- | 26 |
| Recordkeeping requirements----- | 26 |
| Travel rule requirements----- | 26 |
| Responsibilities of beneficiary’s financial institutions----- | 27 |
| Recordkeeping requirements----- | 27 |
| Proceeds delivered in person----- | 27 |
| Proceeds not delivered in person----- | 28 |
| Irretrievability----- | 28 |
| Abbreviations and addresses----- | 28 |
| Customer address----- | 28 |
| Certifications----- | 28 |
| Account closure----- | 29 |
| Verification----- | 29 |
| Requests for AML records by regulator----- | 29 |

| | |
|--|-----------|
| Special due diligence program for foreign correspondent accounts----- | 30 |
| General due diligence----- | 30 |
| Due diligence policies, procedures and controls----- | 30 |
| Risk assessment of foreign financial institutions----- | 30 |
| Monitoring of foreign correspondent accounts----- | 31 |
| Enhanced due diligence----- | 31 |
| Special procedures when due diligence cannot be performed----- | 33 |
| 11. OVERVIEW OF PRIVATE BANKING DUE DILIGENCE PROGRAM (NON-NIGERIANS) --- | 33 |
| Private banking accounts----- | 34 |
| Due diligence program----- | 34 |
| Risk assessment of private banking accounts for Nigerian/non-Nigerian persons----- | 35 |
| Ascertaining source of funds and monitoring account activity----- | 35 |
| Enhanced scrutiny of private banking accounts for senior local/foreign Political figures----- | 36 |
| Identifying senior political figures----- | 37 |
| Special procedures when due diligence cannot be performed----- | 37 |
| 12. OVERVIEW OF SPECIAL MEASURES----- | 37 |
| A. TYPES OF SPECIAL MEASURES----- | 38 |
| Record keeping and reporting of certain financial transactions----- | 38 |
| Information relating to beneficial ownership----- | 38 |
| Information relating to certain payable through accounts----- | 38 |
| Information relating to certain correspondent accounts----- | 38 |
| 13. OVERVIEW OF INTERNATIONAL TRANSPORTATION OF CURRENCY OR MONETARY INSTRUMENTS REPORTING----- | 39 |

| | |
|--|-----------|
| . MONITORING OF OFFICE OF FOREIGN ASSETS CONTROL (OFAC) LIST----- | 39 |
| OFAC reporting----- | 40 |
| OFAC compliance program----- | 40 |
| OFAC risk assessment----- | 41 |
| Internal controls----- | 42 |
| | |
| 14. OVERVIEW AND PROCEDURES FOR CONSOLIDATED AND OTHER TYPES OF AML/CFT COMPLIANCE PROGRAM STRUCTURES | |
| . OVERVIEW OF AML/CFT COMPLIANCE PROGRAM STRUCTURES----- | 45 |
| Structure of the AML/CFT compliance function----- | 46 |
| | |
| . MANAGEMENT AND OVERSIGHT OF THE AML/CFT COMPLIANCE PROGRAM----- | 47 |
| Board of directors----- | 48 |
| Senior management----- | 48 |
| Consolidated AML/CFT compliance programs----- | 49 |
| | |
| . SUSPICIOUS TRANSACTION REPORTING----- | 49 |
| | |
| 15. OVERVIEW OF FOREIGN BRANCHES AND OFFICES OF NIGERIAN FINANCIAL INSTITUTIONS----- | 49 |
| Risk factors----- | 50 |
| Risk mitigation----- | 51 |
| | |
| 16. OVERVIEW OF PARALLEL BANKING----- | 52 |

| | |
|---|-----------|
| Risk factors----- | 52 |
| Risk mitigation----- | 52 |
| 17. OVERVIEW OF CORRESPONDENT ACCOUNTS (DOMESTIC) ----- | 53 |
| ML/FT risk factors----- | 53 |
| Risk mitigation----- | 54 |
| 18. OVERVIEW OF CORRESPONDENT ACCOUNTS (FOREIGN) ----- | 54 |
| Contractual agreements----- | 55 |
| Nested accounts----- | 55 |
| Risk mitigation----- | 56 |
| 19. OVERVIEW OF BULK SHIPMENTS OF CURRENCY----- | 57 |
| Risk factors----- | 57 |
| Risk mitigation----- | 58 |
| Contractual agreements----- | 59 |
| 20. OVERVIEW OF FOREIGN CURRENCY DENOMINATED DRAFTS----- | 60 |
| ML/FT risk factors----- | 60 |
| Risk mitigation----- | 60 |
| 21. OVERVIEW OF PAYABLE THROUGH ACCOUNTS----- | 61 |
| ML/FT Risk Factors----- | 62 |
| Risk mitigation----- | 62 |

| | |
|---|-----------|
| 22. OVERVIEW OF POUCH ACTIVITIES----- | 63 |
| Risk factors----- | 63 |
| Risk mitigation----- | 63 |
| 23. OVERVIEW OF ELECTRONIC BANKING----- | 64 |
| ML/FT risk factors----- | 64 |
| Risk mitigation----- | 65 |
| Remote deposit capture----- | 66 |
| ML/FT risk factors in remote deposit capture----- | 66 |
| Risk mitigation----- | 67 |
| 24. OVERVIEW OF FUNDS TRANSFERS----- | 68 |
| Funds transfer services----- | 68 |
| Society for worldwide interbank financial telecommunication----- | 69 |
| Covers payments----- | 70 |
| Informal value transfer system----- | 70 |
| Payable upon proper identification transactions----- | 70 |
| MI/ft risk factors in funds transfer----- | 70 |
| Risk mitigation----- | 71 |
| 25. OVERVIEW OF AUTOMATED CLEARING HOUSE (ACH) TRANSACTIONS----- | 73 |
| Ach payment systems----- | 73 |
| Third-party service providers----- | 73 |
| Risk factors----- | 74 |
| Risk mitigation----- | 75 |

| | |
|---|-----------|
| 26. OVERVIEW OF ELECTRONIC CASH----- | 76 |
| Risk factors----- | 77 |
| Risk mitigation----- | 77 |
| Prepaid cards/stored value cards----- | 77 |
| Contractual agreements----- | 78 |
| Risk factors----- | 79 |
| Risk mitigation----- | 79 |
| 27. OVERVIEW OF THIRD-PARTY PAYMENT PROCESSORS----- | 80 |
| Risk factors----- | 81 |
| Risk mitigation----- | 81 |
| 28. OVERVIEW OF PURCHASE AND SALE OF MONETARY INSTRUMENTS----- | 83 |
| Risk factors----- | 83 |
| Risk mitigation----- | 83 |
| 29. OVERVIEW OF BROKERED DEPOSITS----- | 84 |
| Risk factors----- | 84 |
| Risk mitigation----- | 84 |
| 30. OVERVIEW OF NON-DEPOSIT INVESTMENT PRODUCTS----- | 86 |
| In house sales and proprietary products----- | 86 |
| Risk factors----- | 87 |
| Risk mitigation----- | 87 |

| | |
|--|------------|
| Networking arrangements----- | 87 |
| 31. OVERVIEW OF INSURANCE PRODUCTS----- | 88 |
| AML/CFT compliance programs and suspicious transaction reporting requirements for insurance companies----- | 89 |
| Risk factors----- | 89 |
| Risk mitigation----- | 90 |
| 32. OVERVIEW OF CONCENTRATION ACCOUNTS----- | 90 |
| Risk factors----- | 90 |
| Risk mitigation----- | 91 |
| 33. OVERVIEW OF PRIVATE BANKING ACTIVITIES----- | 96 |
| Risk factors----- | 97 |
| Risk mitigation----- | 97 |
| Customer risk assessment in private banking----- | 97 |
| Customer due diligence----- | 98 |
| Bearer shares of shell companies----- | 99 |
| Board of directors and senior management oversight of private banking activities----- | 99 |
| 34. OVERVIEW OF TRUST AND ASSET MANAGEMENT SERVICES----- | 100 |
| OBJECTIVE----- | 100 |
| Customer identification program----- | 101 |
| Money laundering and financing of terrorism (ml/ft) risk factors----- | 102 |
| Transfer agent accounts----- | 102 |
| Risk mitigation----- | 102 |
| Customer comparison against various lists----- | 103 |
| Circumstances warranting enhanced due diligence----- | 103 |

| | |
|---|------------|
| 35. OVERVIEW OF EXPANDED EXAMINATION AND PROCEDURES FOR PERSONS AND ENTITIES | |
| . OVERVIEW OF NON-RESIDENT ALIENS AND FOREIGN INDIVIDUALS----- | 104 |
| Risk factors of NRA account holder----- | 104 |
| Risk mitigation----- | 104 |
| 36. OVERVIEW OF POLITICALLY EXPOSED PERSONS----- | 105 |
| Risk factors----- | 107 |
| Risk mitigation----- | 107 |
| 37. OVERVIEW OF EMBASSY AND FOREIGN CONSULATE ACCOUNTS----- | 108 |
| Risk factors----- | 109 |
| Risk mitigation----- | 110 |
| 38. OVERVIEW OF DESIGNATED NON-FINANCIAL INSTITUTIONS----- | 110 |
| Risk factors----- | 110 |
| Risk mitigation----- | 111 |
| MSB risk assessment----- | 112 |
| MSB risk mitigation----- | 113 |
| Factors that may reduce or mitigate the risk in some MSB accounts----- | 113 |
| MSB due diligence expectations----- | 114 |
| 39. OVERVIEW OF PROFESSIONAL SERVICE PROVIDERS----- | 115 |
| Risk factors----- | 115 |
| Risk mitigation----- | 116 |

| | |
|---|------------|
| 40. OVERVIEW OF NON-GOVERNMENTAL ORGANIZATIONS AND CHARITIES----- | 116 |
| Risk factors----- | 116 |
| Risk mitigation----- | 116 |
| 41. OVERVIEW OF BUSINESS ENTITIES (DOMESTIC AND FOREIGN) ----- | 117 |
| Domestic business entities----- | 117 |
| Foreign business entities----- | 118 |
| International business corporations----- | 118 |
| Private investment companies----- | 119 |
| Risk factors----- | 119 |
| Indicators of potentially suspicious activity commonly associated with Shell company activity----- | 120 |
| Risk mitigation----- | 120 |
| 42. OVERVIEW OF CASH-INTENSIVE BUSINESSES----- | 122 |
| Risk factors----- | 122 |
| Risk mitigation----- | 122 |

AML/CFT RBS REGULATION FOR FINANCIAL INSTITUTIONS F/Is

1. Background

It is MLPA, 2004 and CBN AML/CFT Regulation, 2009 that establish the requirements for record-keeping and reporting by designated non-financial institutions, businesses & professions, banks and other financial institutions to regulatory authorities. Relevant provisions of the law and regulation were designed to **help identify the source, volume and movement of currency and other monetary instruments transported or transmitted into or out of Nigeria, or deposited in financial institutions in the country.**

The enabling Act & Regulation under reference seek to achieve the objective by requiring individuals, banks and other financial institutions to **render politically exposed persons returns and currency transaction reports (CTRs)** to the CBN (AML/CFT Office in Financial Policy & Regulation Department) and Nigerian Financial Intelligence Unit (NFIU); **to properly identify persons conducting transactions and to maintain a paper trail** by keeping appropriate records of their financial transactions. Should the need arise, these records will enable law enforcement and regulatory agencies to pursue investigations of criminal, tax & regulatory violations, and provide useful evidence in prosecuting money laundering and other financial crimes.

The MLPA, 2004 and CBN AML/CFT Regulation, 2009 apply equally to all banks, other financial institutions and persons that are under the regulatory purview of the CBN. The law also imposes criminal liability on a person or financial institution that knowingly assists in the laundering of money or fails to report suspicious transactions conducted through it. The CBN AML/CFT Regulation also directs financial institutions to establish and maintain procedures reasonably designed to ensure and monitor compliance with the reporting and record-keeping requirements of the MLPA, 2004.

2. Suspicious Transaction Report

A financial institution is required to render a Suspicious Transaction Report (STR) to NFIU and inform the CBN of same whenever it detects a known or suspected criminal violation of MLPA or a suspicious transaction related to money laundering activity or a violation of other laws & regulations.

The EFCC Act criminalizes the financing of terrorism. CBN AML/CFT Regulation, 2009 has also augmented the existing MLPA legal framework by strengthening customer identification procedures, prohibiting financial institutions from engaging in business with foreign shell banks, requiring financial institutions to have due diligence procedures (in some cases, have enhanced due diligence (EDD) procedures for foreign

correspondent and private banking accounts) and improving information sharing between financial institutions and the law enforcement agencies (LEAs) and regulators.

3. MLPA & CBN AML/CFT Regulation

The Laws and Regulation provide for

- i. Financial institutions to have AML/CFT Program;
- ii. Civil and criminal penalties for money laundering to be imposed;
- iii. CBN to impose sanctions for AML/CFT infractions committed by institutions and persons in course of transactions;
- iv. Financial institutions to facilitate access to records and give prompt response to regulatory requests for information; and
- v. Financial institutions to consider their AML/CFT records when reviewing mergers, acquisitions and other applications for business combinations.

Regulatory Agencies in Nigeria Financial Sector

The regulatory agencies are responsible for the oversight of the various financial institutions operating in Nigeria, including foreign-owned subsidiaries of Nigerian banks and other financial institutions. While the Corporate Affairs Commission (CAC) is charged with the registration of banks and other financial institutions, the CBN is responsible for licensing them. SEC & NAICOM license the capital market operators and insurance businesses, respectively. The enabling statutes of these regulators require them to review the AML/CFT Compliance Program at each examination of the regulated institutions. They are also required to use the authority granted them under their Acts to enforce compliance with appropriate rules and regulations, including compliance with AML/CFT regulations.

These agencies require each institution under their supervisory purview to establish and maintain AML/CFT Compliance Program. **The program guards against money laundering and terrorist financing transactions and ensures compliance with and implementation of money laundering laws and regulations.** Financial institutions are required to take reasonable and prudent steps to combat money laundering and terrorist financing and minimize their vulnerability to the risk associated with such activities.

Financial institutions that have damaged their reputations will be required to pay civil financial penalties for failing to implement adequate controls within their institutions as a result of non-compliance with the MLPA & AML/CFT Regulation, 2009. In addition, AML/CFT assessment is also required as part of application process, since AML/CFT concerns will have an impact on the financial institution's strategic plan. For this reason,

the CBN shall accord high supervisory priority and provide guidance that assists the regulated institutions in complying with the MLPA & AML/CFT Regulation.

The CBN shall ensure that the institutions under its supervisory purview understand the importance of having an effective AML/CFT Compliance Program in place. Managements of the regulated institutions are also required to be vigilant & ensure they have AML/CFT Compliance Program, especially as business grows and new products and services are introduced. To this end, an evaluation of the institution's AML/CFT Compliance Program and its compliance with the regulatory requirements of the AML/CFT Regulation must be made an integral part of the supervisory process by both the CBN and the institutions.

As part of a strong AML/CFT Compliance Program, the CBN shall ensure that a financial institution has policies, procedures and processes to identify and report suspicious transactions to NFIU and inform the CBN and the appropriate law enforcement agencies as required by the AML/CFT Regulation. The Bank Examiners' supervisory processes will include assessing whether or not the financial institution has established the appropriate policies, procedures and processes based on its money laundering risk in order to identify and report suspicious transaction and that the AML/CFT reports produced provide sufficient details to the law enforcement agencies to make such reports useful for further investigation.

The CBN has specific powers to impose controls on transactions and freeze assets held within Nigerian jurisdiction and sanctions are based on the provisions of Nigeria Laws, United Nations and other international mandates. They are multilateral in scope and involved close cooperation with allied governments and the financial institutions concerned.

4. Money Laundering and Terrorist Financing

The MLPA & AML/CFT Regulation, 2009 are intended to safeguard Nigerian financial system and other financial institutions that make up the system from the abuses of financial crime, including money laundering, terrorist financing and other illicit financial transactions. Money laundering and terrorist financing are financial crimes with potentially devastating social and financial effects to the Nigerian and word economy.

From the profits of the narcotics trafficker to the assets looted from government coffers by dishonest foreign & local officials, criminal proceeds have the power to corrupt and ultimately destabilize communities or entire economy. Terrorist networks are able to facilitate their activities if they have financial means and access to the financial system. In both money laundering and terrorist financing, criminals can exploit loopholes and other weaknesses in the legitimate financial system to launder criminal proceeds,

finance terrorism or conduct other illegal activities in order to ultimately hide the actual purpose of their activity.

Financial institutions are required to develop, implement and maintain effective AML/CFT Programs that address the ever-changing strategies of money launderers and terrorists who attempt to gain access to the Nigerian financial system. A sound AML/CFT Compliance Program is critical in deterring and preventing these types of activities at or through banks and other financial institutions.

5. OVERVIEW OF ML/FT RISK ASSESSMENT

Customers and Entities

Any type of account is potentially vulnerable to money laundering or terrorist financing. By the nature of their business, occupation or anticipated transaction activity, certain customers and entities may pose specific risks. At this stage of the risk assessment process, it is essential that the financial institution exercises judgment and neither define nor treat all members of a specific category of customer as posing the same level of risk.

In assessing **customer risk**, financial institutions are required to consider other variables such as **services sought and geographic locations. Guidance and discussion on specific customers and entities that are detailed below may be necessary:**

- i. Foreign financial institutions, including banks and foreign money services providers (e.g. currency exchanges and money transmitters).
- ii. Non-bank financial institutions (e.g. money services businesses; casinos and card clubs; brokers/dealers in securities; and dealers in precious metals, stones or jewels).
- iii. Senior foreign & domestic political figures, their immediate family members and close associates [collectively known as politically exposed persons (PEPs)].
- iv. Non-resident alien (NRA) and accounts of foreign individuals.
- v. Foreign corporations and domestic business entities, particularly offshore corporations (such as domestic shell companies and private investment companies (PIC) and international business corporations (IBC)) located in higher-risk geographic locations.
- vi. Deposit brokers particularly foreign deposit brokers.

- vii. Cash-intensive businesses (e.g. convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs and parking garages).
- viii. Non-governmental organizations and charities (foreign and domestic).
- ix. Professional service providers (e.g. attorneys, accountants, doctors or real estate brokers).

Geographic Locations

Identifying geographic locations that may pose a higher risk is essential to a financial institution's AML/CFT Compliance Program. Financial institutions are required to understand and evaluate the specific risks associated with doing business in, opening accounts for customers from or facilitating transactions involving certain geographic locations. However, **geographic risk alone does not necessarily determine a customer's or transaction's risk level, either positively or negatively.**

Analysis of Specific Risk Categories

The second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage. It is to help assess more accurately the associated ML/FT risk involved. This step involves evaluating data pertaining to the financial institution's activities (e.g. the number of domestic and international funds transfers; private banking customers; foreign correspondent accounts; PTAs and domestic and international geographic locations of the institution's business area and customer transactions) in relation to customer identification program (CIP) and customer due diligence (CDD) information.

The level and sophistication of analysis may vary from one financial institution to another. The detailed analysis is important because within any type of product or category of customer there will be account holders that pose varying levels of risk.

This step (in the risk assessment process) gives the institutions management a better understanding of its institution's risk profile in order to develop the appropriate policies, procedures and processes to mitigate the overall risk. Specifically, **the analysis of the data pertaining to the financial institution's activities should consider, as appropriate, the following factors:**

- i. Purpose of the account.
- ii. Actual or anticipated activity in the account.
- iii. Nature of the customer's business/occupation.
- iv. Customer's location.
- v. Types of products and services used by the customer.

The value of a two-step risk assessment process is illustrated in the following example of data collected in the **first step of the risk assessment process which reflects that a financial institution sends out 100 international funds transfers per day:**

- i. Further analysis may show that approximately 90 percent of the funds transfers are **recurring well-documented transactions for long-term customers;** and
- ii. On the other hand, the analysis may show that 90 percent of these transfers **are non-recurring or are for non-customers.**

While the numbers are the same for the two examples above, the overall risks are different. As illustrated above, the institution's customer identification program (CIP) and customer due diligence (CDD) information must play important roles in this process.

Developing the Financial Institution's AML/CFT Compliance Program Based Upon its Risk Assessment

Financial Institution's management is required to structure its institution's AML/CFT Compliance Program to adequately address its risk profile as identified by its risk assessment. Management should therefore understand its financial institution's ML/FT risk exposure and develop the appropriate policies, procedures and processes to monitor and control its ML/FT risks. For example, **the financial institution's monitoring systems should be able to identify, research and report suspicious activity. Such process must be risk-based with particular emphasis on higher-risk products, services, customers, entities and geographic locations as identified by the institution's ML/FT risk assessment.**

Note that independent testing (audit) is required to review the financial institution's risk assessment for reasonableness. Additionally, management is also required to consider the staffing resources and the level of training that are necessary to promote adherence with these policies, procedures and processes. For those financial institutions that assume a higher-risk AML/CFT profile, management should be required to provide a **more robust AML/CFT Compliance Program** that specifically monitors and controls the higher risks accepted by the management and board.

Consolidated AML/CFT Compliance Risk Assessment

Financial institutions that implement a consolidated or partially consolidated AML/CFT Compliance Program are required to **assess risk both individually within business**

lines and across all activities and legal entities. Aggregating ML/FT risks on a consolidated basis for larger or more complex institutions may enable the organization to better identify risks and risk exposures within and across specific lines of business or product categories. Consolidated information also assists senior management and the board of directors in understanding and appropriately mitigating risks across the institution.

To avoid having an outdated understanding of the ML/FT risk exposures, the financial institution should be required to continually reassess its ML/FT risks and communicate with its business units, functions and legal entities. The identification of ML/FT risks or deficiency in one area of business may indicate concerns elsewhere in the institution. This therefore requires the management's attention to identify and control them.

Updating of Risk Assessment by Financial Institution

An effective AML/CFT Compliance Program must be able to control the risks associated with the institution's products, services, customers, entities and geographic locations. Therefore, an effective risk assessment is required to be an ongoing process, not a one-time exercise.

Management is required to update its risk assessment to identify changes in the financial institution's risk profile when it is necessary, especially **when new products and services are introduced, existing products and services change, higher-risk customers open and close accounts or the financial institution expands through mergers and acquisitions.**

In the absence of such changes and in the spirit of sound practice, financial institutions are required to periodically reassess their ML/FT risks at least every 12 to 18 months.

Minimum Requirement of AML/CFT Compliance

The program should contain the following:

- i. A system of internal controls to ensure on-going compliance.
- ii. Independent testing of AML/CFT compliance.
- iii. Designate an individual or individuals responsible for managing AML/CFT compliance (Chief compliance officer).
- iv. Training for appropriate personnel.

Internal Controls

The board of directors, acting through senior management, is ultimately responsible for ensuring that the financial institution maintains an effective AML/CFT internal control

structure, including suspicious activity monitoring and reporting. The board of directors and management should create a culture of compliance to ensure staff adherence to the financial institution's AML/CFT policies, procedures and processes.

Internal controls are the institution's policies, procedures and processes designed to limit and control risks and to achieve compliance with the MPLA and CBN AML/CFT Regulation 2009.

The level of sophistication of the internal controls should be commensurate with the size, structure, risks and complexity of the financial institution. Large complex financial institutions are more likely to implement departmental internal controls for AML/CFT compliance.

Departmental internal controls typically address risks and compliance requirements unique to a particular line of business or department and are part of a comprehensive AML/CFT Compliance Program.

Internal controls should:

- i. Identify financial institution's **operations** (i.e. products, services, customers, entities and geographic locations) **that are more vulnerable to abuse by money launderers and criminals**. They should ensure that the institution provides for periodic updates to its risk profile and has AML/CFT Compliance Program that is tailored to manage risks.
- ii. Be such that the **board of directors or its committee thereof and senior management are informed of** AML/CFT compliance initiatives, identified compliance deficiencies and corrective action taken, and the directors and senior management should be notified of returns rendered to the regulatory authorities.
- iii. **Identify a person or persons responsible for AML/CFT compliance.**
- iv. Provide for **program continuity by way of back-up** in personnel and information storage & retrieval in cases of changes in management or employee composition or structure.
- v. Provide for meeting all regulatory recordkeeping and reporting requirements, implement all recommendations for AML/CFT compliance and provide for timely updates in response to changes in regulations.
- vi. Cover the implementation of risk-based CDD policies, procedures and processes
- vii. Identify reportable transactions and that all the required reports are accurately rendered promptly and these include STRs, PEPs, CTRs and CTR-exemptions (if any). Financial institutions are required to centralize their review and report-remittance functions within a unit in the branches and head-offices.
- viii. Provide for dual controls and the segregation of duties as much possible. For example, employees that complete the reporting forms (such as STRs, CTRs

- and CTR-exemptions) generally should not also be responsible for taking the decision to file the reports or grant the exemptions.
- ix. Provide sufficient controls and systems for rendering CTRs and CTR exemptions.
 - x. Provide sufficient controls and systems of monitoring timely detection and reporting of suspicious activity.
 - xi. Provide for adequate supervision of employees that handle currency transactions, complete reporting formats, grant exemptions, monitor suspicious activity or engage in any other activity covered by the MLPA, AML/CFT Regulation and other guidelines.
 - xii. Incorporate MLPA & AML/CFT Regulation-compliance into the job descriptions and performance evaluations of financial institution personnel, as appropriate.
 - xiii. Provide for the training of employees to be aware of their responsibilities under the AML/CFT Regulations and internal policy guidelines.

Independent Testing

Independent testing (audit) should be conducted by the internal audit department, external auditors, consultants or other qualified independent parties. While the frequency of audit is not specifically defined in any statute, **a sound practice is for the financial institution to conduct independent testing generally every 12 to 18 months or commensurate with the ML/FT risk profile of the institution.**

Financial institutions that do not employ outside auditors, consultants or have internal audit departments **may comply with this requirement by using qualified persons who are not involved in the function that is tested.**

The persons conducting the AML/CFT testing should report directly to the board of directors or to a designated board committee consisting primarily or completely of outside directors.

Those persons responsible for conducting an objective independent evaluation of the written AML/CFT Compliance Program should perform testing for specific compliance with the MLPA, AML/CFT Regulation and other related requirements. They are required to also evaluate pertinent management information systems (MIS). The audit has to be risk-based and must evaluate the quality of risk management for all the financial institution's operations, departments and subsidiaries.

Risk-based Audit Programs will vary depending on the institution's size, complexity, scope of activities, risk profile, quality of control functions, geographic diversity and use of technology. An effective risk-based auditing program will **cover all of the institution's activities.** The frequency and depth of each audit activity will vary according to the activity's risk assessment.

It should be noted that the risk-based auditing will enable the board of directors and auditors to use the financial institution's risk assessment to **focus its scope of audit on the areas of greatest concern**. The testing should assist the board of directors and management in **identifying areas of weakness or areas where there is a need for enhancements or stronger controls**.

Independent testing should (at a minimum) include:

- i. The evaluation of the overall adequacy and effectiveness of the AML/CFT Compliance Program, including policies, procedures and processes. This evaluation will contain an **explicit statement about the AML/CFT compliance program's overall adequacy and effectiveness and compliance with applicable regulatory requirements**. At the very least, the audit should contain sufficient information for the reviewer (e.g. an Examiner, review auditor or NFIU officer) to reach a conclusion about the overall quality of the AML/CFT Compliance Program.
- ii. A review of the financial institution's risk assessment for reasonableness given the institution's risk profile (products, services, customers, entities and geographic locations).
- iii. Appropriate risk-based transaction testing to verify the financial institution's adherence to the MPLA and CBN AML/CFT Regulation, 2009 recordkeeping and rendition of returns requirements on PEPs, STRs, CTRs and CTR-exemptions and information sharing requests.
- iv. An evaluation of management's efforts to resolve violations and deficiencies noted in previous audits and regulatory examinations, including progress in addressing outstanding supervisory actions (if applicable).
- v. A review of staff training for adequacy, accuracy and completeness.
- vi. A review of the effectiveness of the suspicious transaction monitoring systems (are they manual, automated or a combination?) used for AML/CFT compliance. **Related reports may include, but are not limited to:**
 - a. Suspicious transaction monitoring reports.
 - b. Large currency aggregation reports.
 - c. Monetary instrument records.
 - d. Funds transfer records.
 - e. Non-sufficient funds (NSF) reports.
 - f. Large balance fluctuation reports.
 - g. Account relationship reports.
 - h. An assessment of the overall process for identifying and reporting suspicious transaction, including a review of filed or prepared STRs to determine their accuracy, timeliness, completeness and effectiveness of the institution's policy.

- vii. An assessment of the integrity and accuracy of MIS used in the AML/CFT Compliance Program. MIS includes reports used to identify and extract data on the large currency transactions, aggregate daily currency transactions, funds-transfer transactions, monetary instrument sales transactions and analytical and trend reports.

The auditors' report should include their documentation on the scope of the audit, procedures performed, transaction testing completed and findings of the review. All audit documentation and work-papers should be made available for the Examiner to review. Any violations, policy or procedures exceptions or other deficiencies noted during the audit should be included in the audit report and reported to the board of directors or its designated committee in a timely manner.

The board or designated committee and the audit staff are required to track the deficiencies observed in the auditors' report and document the corrective actions recommended and taken.

Chief Compliance Officer

The institution's board of directors is required to designate a qualified individual that must not **be less than a General Manager to serve as the Chief Compliance Officer (CCO)**. The CCO is responsible for the coordinating and monitoring of day-to-day AML/CFT compliance by the institution. The CCO is also charged with managing all aspects of the AML/CFT Compliance Program and with managing the institution's adherence to the MLPA, AML/CFT Regulation and other AML/CFT Requirements. However, it is the board of directors that is ultimately responsible for the institution's AML/CFT compliance.

As the title of the individual responsible for overall AML/CFT compliance is of importance, his/ her level of authority and responsibility within the financial institution is also critical. Though the CCO may delegate the AML/CFT duties to other employees, he/she will be held responsible for the overall AML/CFT compliance by the institution. The board of directors is responsible for ensuring that the CCO has sufficient authority and resources (monetary, physical and personnel) to administer an effective AML/CFT Compliance Program based on the institution's risk profile.

The CCO should be fully knowledgeable of the MLPA, AML/CFT Regulation and all related requirements. The CCO should also understand the institution's products, services, customers, entities, geographic locations and the potential money laundering and terrorist financing risks associated with these activities. The appointment of a CCO is not sufficient to meet the regulatory requirement if that person does not have the expertise, authority or time to satisfactorily carry out the job efficiently and effectively.

Confirm that the line of communication allows the CCO to regularly apprise the board of directors and senior management of ongoing compliance with AML/CFT regime of the institution. Ensure that pertinent MLPA-related information, including the reporting of STRs rendered to NFIU are reported to the board of directors or an appropriate board committee so that these individuals can make informed decisions about the overall AML/CFT compliance of the institution. Ensure also that the CCO is responsible for carrying out the directives of the board and ensuring that employees adhere to the institution's AML/CFT policies, procedures and processes.

Training

Financial institutions are required to ensure that appropriate personnel are trained in applicable aspects of the MLPA & AML/CFT Regulation. The training should cover the **regulatory requirements and the institution's internal AML/CFT policies, procedures and processes.**

At a minimum, the financial institution's training program must provide training for all personnel whose duties require knowledge of the MLPA & AML/CFT Regulation. The training should be tailored to the person's specific responsibilities. In addition, an overview of the AML/CFT requirements typically should be given to new staff during employee orientation. Training should encompass information related to **applicable business lines such as trust services, international and private banking.**

The CCO should receive periodic training that is relevant and appropriate given changes to regulatory requirements as well as the activities and overall ML/FT risk profile of the institution.

The board of directors and senior management should be informed of changes and new developments in the MLPA and AML/CFT Regulation, other guidelines and directives, and regulations by other agencies. While the board of directors may not require the same degree of training as the institution operations personnel, they need to understand the importance of AML/CFT regulatory requirements, the ramifications of non-compliance and the risks posed to the institution. Without a general understanding of the MLPA & AML/CFT Regulation, the board of directors cannot adequately provide AML/CFT oversight, approve AML/CFT policies, procedures and processes or provide sufficient AML/CFT resources.

Training should be on-going and incorporate current developments and changes to the MLPA, AML/CFT Regulation and other related guidelines. Changes to internal policies, procedures, processes and monitoring systems should also be covered during training. The training program should reinforce the importance that the board and senior management place on the institution's compliance with the MLPA & AML/CFT Regulation and ensure that all employees understand their roles in maintaining an effective AML/CFT Compliance Program.

Examples of money laundering activity and suspicious transaction monitoring and reporting can and should be tailored to each individual audience. For example, training for tellers should focus on examples involving large currency transactions or other suspicious transactions while training for the loan department should provide examples involving money laundering through lending arrangements.

Financial institutions are required to document their training programs. Training and testing materials, the dates of training sessions and attendance records should be maintained by the institution and be made available for the Bank Examiner to review.

6. OVERVIEW OF PROCEDURES FOR REGULATORY REQUIREMENTS AND RELATED TOPICS

Overview of Customer Identification Program

All financial institutions are required to have a written Customer Identification Program (CIP). Each financial institution should **implement a written CIP** that is appropriate for its size and type of business and that includes certain minimum requirements. The CIP must be incorporated into the institution's AML/CFT Compliance Program which is subject to approval by the institution's board of directors.

The implementation of a CIP by the financial institution's subsidiaries is appropriate as a matter of safety, soundness and protection from reputation risks. Domestic subsidiaries (other than functionally regulated subsidiaries that are subject to separate CIP rules) of financial institutions should comply with the CIP rule that applies to the parent institution when opening an account.

The CIP is intended to enable the financial institution to form a reasonable belief that it knows the true identity of each customer. The CIP must include account opening procedures that specify the identifying information that will be obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer.

Each financial institution is required to conduct a risk assessment of its customer base and product offerings. To determine the risks involved it must consider:

- i. The types of accounts offered by it.
- ii. The institution's methods of opening accounts.
- iii. The types of identification information available.
- iv. The institution's size, location and customer base, including types of products and services used by the customers in different geographic locations.

Verification through Documents

A financial institution using documentary methods to verify a customer's identity must have procedures that set forth the minimum acceptable documentation. The identification **must provide evidence of a customer's nationality or residence and bear a photograph or similar safeguard.** Examples include a driver's licence or international passport. However, other forms of identification may be used if they enable the institution to form a reasonable belief that it knows the true identity of the customer. Nonetheless, given the availability of counterfeit and fraudulently obtained documents, a financial institution is encouraged to review more than a single document to ensure that it has a reasonable belief that it knows the customer's true identity. For a "person" other than an individual (such as a corporation, partnership or trust), the institution should obtain documents showing the legal existence of the entity. Such documents include certified Memorandum & Articles (Memart) of Association of the incorporation, an un-expired government-issued business licence, a partnership agreement or a trust instrument.

Verification through Non-documentary Methods

Financial institutions are not advised to use non-documentary methods to verify a customer's identity. However, a financial institution using non-documentary methods to verify a customer's identity must have procedures that set forth the methods to be used by the institution.

Record-keeping and Retention Requirements

A financial institution's CIP must include record-keeping procedures. At a minimum, the institution must retain the identification information such as name, address, date of birth for an individual, tax identification number (TIN) and any other information required by the CIP which are obtained at account opening for a period of five years after the account is closed. For credit cards, the retention period is also five years after the account closes or becomes dormant.

The financial institution is required also keep a description of the following for five years after the record was made:

- i. Any document that was relied on to verify identity, noting the type of document, the identification number, the place of issuance and the date of issuance and expiration date (if any).
- ii. The method and the results of any measures undertaken to verify identity.
- iii. The results of any substantive discrepancy discovered when verifying the identity.

Comparison with Terrorist Lists

The CIP must include procedures for determining whether existing or potential customer appears on any list of known or suspected terrorists or terrorist organizations. As often as possible and in accordance with the requirements of the AML/CFT Regulation and other related requirements on the subject, financial institutions are required to compare customer names against the list of terrorists after the account opening procedure is completed.

Adequate Customer Notice

The CIP must include procedures and evidence in which the financial institution has provided customers with adequate notice for request of information to verify their identities. The notice must generally describe the financial institution's identification requirements and this should be provided in a manner that is reasonably designed to allow a customer to view it or otherwise receive the notice before the account is opened. **Examples include posting the notice in the lobby, on a Web site or within loan application documents. Sample of such notice is provided below:**

7. IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT

To help the government fight the funding of terrorism and money laundering activities, the law and regulation require all financial institutions to obtain, verify and record information that identifies each person who opens an account. What this means is that when you open an account, we will ask for your name, address, date of birth and other information that will allow us identify you. We may also ask to see your driver's licence, international passport, TIN, National Identity Card, Voter Registration Card or other identifying documents.

Reliance on another Financial Institution

A financial institution is **permitted** to rely on another financial institution (including an affiliate) to perform some or all of the elements of the CIP. If such reliance is addressed in the CIP, the following criteria must be met:

- i. The relied-upon financial institution must be subject to a rule that makes it mandatory to implement the AML program requirements.
- ii. The customer has an account or is opening an account at the institution and at the other functionally regulated institution.
- iii. Such reliance must be reasonable under the circumstances.
- iv. The financial institution must enter into a contract, requiring the other financial institution to certify annually to the beneficiary financial institution that the agent-institution has implemented its own AML Program and that it will perform (or its agent will perform) the specified requirements of the institution's CIP.

Use of Third Parties

The CIP rule does not alter a financial institution's authority to use a third party such as an agent or service provider to perform services on its behalf. Therefore, a financial institution is permitted to arrange for a third party such as a Car Dealer or Mortgage Broker to act as its agent in connection with a loan for purpose of verifying the identity of its customer. The financial institution can also arrange for a third party to maintain its records. As with any other responsibility performed by a third party, the financial institution is ultimately responsible for that third party's compliance with the requirements of its CIP. As a result, financial institution should establish adequate controls and review procedures for such relationships.

Other Legal Requirements

Nothing in the CIP rule relieves a financial institution of its obligations under any provision of the MLPA, AML/CFT Regulation, other laws, rules and regulations, particularly with respect to provisions concerning information that must be obtained, verified or maintained in connection with any account or transaction.

Inquiries and Requests by PEPs

Financial institutions should establish policies, procedures and processes for identifying PEPs' requests, monitoring their transaction activity when appropriate, identifying unusual or potentially suspicious transaction related to those subjects and filing, as appropriate, STRs related to them.

Examiners should review the adequacy and effectiveness of the policies, procedures and processes of identifying PEPs' requests, monitoring their transaction activity when appropriate, identifying unusual or potentially suspicious transaction related to them, filing as appropriate, STRs related to the subjects.

Funds transfer records

The MLPA 2004 and CBN AML/CFT Regulation 2009 require financial institutions to maintain records of funds transfer in amounts of N1 million & above for individuals; and N2 million & above for corporate bodies. Periodic review of this information can assist financial institutions in identifying patterns of unusual activity. A periodic review of the funds transfer records in financial institutions with low funds transfer activity is usually sufficient to identify unusual activity. For financial institutions with more significant funds transfer activity, use of spreadsheet or vendor software is an efficient way to review funds transfer activity for unusual patterns. Most vendor software systems include standard suspicious transaction filter reports. These reports typically focus on identifying certain higher-risk geographic locations and larger currency funds transfer transactions for individuals and businesses.

Each institution should establish its own filtering criteria for both individuals and businesses. Non customer funds transfer transactions and payable upon proper identification (PUPID) transactions should be reviewed by Examiners for unusual activity. Activities identified during these reviews should be subjected to additional research to ensure that identified activity is consistent with the stated account purpose and expected activity. When inconsistencies are identified, financial institutions may need to conduct a global relationship review to determine if a STR is warranted.

Monetary instrument records

Keeping of record for sale of monetary instrument is a requirement of the MLPA and CBN AML/CFT Regulation 2009. Such records can assist the financial institution in identifying possible currency structuring through the purchase of cashier's cheques, official bank/financial institution cheques, money orders, or traveller's cheques in amounts of USA \$10,000 or its equivalent. A periodic review of these records can also help identify frequent purchasers of monetary instruments and common payees. Reviews for suspicious transaction should **encompass activity for an extended period of time (30, 60, 90 days) and should focus on, among other things, identification of commonalities, such as common payees and purchasers, or consecutively numbered purchased monetary instruments.**

Surveillance Monitoring (Automated Account Monitoring)

A surveillance monitoring system (sometimes referred to as an automated account monitoring system) can cover multiple types of transactions and use various rules to identify potentially suspicious transaction. In addition, many can adapt over time based on historical activity, trends or internal peer comparison. These systems typically use computer programs to identify individual transactions, patterns of unusual activity or deviations from expected activity. These systems can capture a wide range of account activity, such as deposits, withdrawals, funds transfers, automated clearing house (ACH) transactions and automated teller machine (ATM) transactions, directly from the financial institution's core data processing system.

STR Completion and Filing

STR completion and filing are a critical part of the STR monitoring and reporting process. Appropriate policies, procedures and processes should be in place to ensure that STR forms are filed in a timely manner, are complete and accurate, and that the narrative provides a sufficient description of the activity reported as well as the basis for filing.

8. OVERVIEW OF CURRENCY TRANSACTION REPORTING

A financial institution is required to file Currency Transaction Report (CTR) for each transaction in cash (deposit, withdrawal, exchange or other payment or transfer) of N1,000,000 & above or N5,000,000 & above for individuals or corporate bodies respectively **through, from or to the financial institution**. All types of currency transactions are to be reported, there are no "exempt persons".

Aggregation of Currency Transactions

Multiple cash transactions totaling more than N1,000,000 or N5,000,000 and above for individuals or corporate bodies respectively during any one business day are treated as a single transaction if the financial institution has knowledge that they are by or on behalf of the same person. Transactions throughout the financial institution should be aggregated when determining multiple transactions. Types of currency transactions subject to reporting requirements individually or by aggregation include but are not limited to **denomination exchanges, individual retirement accounts (IRA), loan payments, automated teller machine (ATM) transactions, purchases of certificates of deposit, deposits and withdrawals, funds transfers paid for in currency and monetary instrument purchases**. Financial institutions are strongly encouraged to develop systems necessary to aggregate currency transactions throughout the institution. Management should ensure that an adequate system exists and is implemented that will appropriately report currency transactions subject to the CBN AML/CFT Regulation 2009 requirement.

Filing Time Frames and Record Retention Requirements

A completed CTR is required to be filed (manually or electronically) with NFIU & AML/CFT Office, CBN **within 7 days after the date of the transaction**. The financial institution must retain copies of CTRs for five years from the date of the report.

CTR Back-filing

If a financial institution has failed to file CTRs on reportable transactions, the institution is required to file the un-filed CTRs immediately.

Information Sharing Between Law Enforcement and Financial Institutions

Search Requirements

Upon receiving an information-request, a financial institution is required to conduct a one-time search of its records to identify accounts or transactions of a named suspect. **Unless otherwise instructed by an information-request, financial institutions**

must search their records for current accounts, accounts maintained during the preceding 12 months and transactions conducted outside of an account by or on behalf of a named suspect during the preceding six months. The financial institution must search its records and report any positive matches to CBN/NFIU within seven (7) days, unless otherwise specified in the information-request. If a financial institution identifies any account or transaction, it must report to the CBN/NFIU that it has a match. Relevant details are required to be provided to CBN/NFIU in addition to the fact that the financial institution has found a match. Where no match is found, a nil report must be submitted within the deadline. The institution is forbidden to keep silence or provide no response.

A financial institution may provide subject lists to a third-party service provider or vendor to perform or facilitate record searches as long as the institution takes the necessary steps, through the use of an agreement or procedures to ensure that the third party safeguards and maintains the confidentiality of the information.

If a financial institution that receives the subject lists fails to perform or complete searches on one or more information-request received during the previous 12 months, it must immediately obtain these prior requests from CBN/NFIU and perform a retroactive search of its records.

A financial institution is not required to perform retroactive searches in connection with information sharing requests that were transmitted more than 12 months before the date upon which it discovers that it failed to perform or complete searches on prior information requests. Additionally, in performing retroactive searches a financial institution is not required to search records created after the date of the original information request.

Restrictions and Confidentiality

Financial institutions should develop and implement comprehensive policies, procedures and processes for responding to requests. A financial institution may use the required information rendered to CBN/NFIU to determine whether to establish or maintain an account or engage in a transaction, or to assist in its AML/CFT compliance. While the subject-list could be used to determine whether to establish or maintain an account, CBN/NFIU strongly discourages financial institutions from using this as the sole factor in reaching a decision to do so, unless the request specifically states otherwise.

Subject-lists are not permanent "watch lists". They generally relate to one-time inquiries and could not be updated or corrected if an investigation is dropped, a prosecution is declined, or a subject is exonerated. Furthermore, such names do not necessarily correspond to convicted or indicted persons. **A subject need only be "reasonably suspected" based on credible evidence of engaging in terrorist acts or money**

laundering. Moreover, CBN/NFIU advises that inclusion of a name on subject-list should not be the sole factor used to determine whether to file STR. Financial institutions are required to establish a process for determining when and if a STR should be filed.

Actions taken pursuant to information provided in a request from CBN/NFIU do not affect a financial institution's obligations to comply with all of the rules and regulations of **MLPA 2004 and CBN AML/CFT Regulation 2009** nor do they affect a financial institution's obligations to respond to any legal process. Additionally, actions taken in response to a request do not relieve a financial institution of its obligation to file a STR and immediately notify LEA, if necessary, in accordance with applicable laws and regulations.

A financial institution must not disclose to any person (other than to CBN/NFIU, the institution's primary regulator or the LEA on whose behalf CBN/NFIU is requesting information) the fact that CBN/NFIU has requested or obtained information. A financial institution should designate one or more points of contact for receiving information-requests. **An affiliated group of financial institutions may establish one point of contact to distribute the subject-list to respond to requests.** However, the subject-lists cannot be shared with any foreign office, branch or affiliate (unless the request specifically states otherwise). The lists cannot be shared with affiliates or subsidiaries of financial institutions' holding companies, if the affiliates or subsidiaries are not financial institutions.

Each financial institution must maintain adequate procedures to protect the security and confidentiality of requests from CBN/NFIU. The procedures to ensure confidentiality will be considered adequate if the financial institution applies procedures similar to those it has established to comply with regulatory requirements in order to **protect its customers' non-public personal information.** Financial institutions may keep a log of all requests received and of any positive matches identified and reported to CBN/NFIU

Documentation

Additionally, documentation of how all the required searches were conducted is essential. **A financial institution may maintain copies of the cover page of the request on which it signed-off that the records were checked, the date of the search and search results (positive or negative).** For positive matches with subject-lists received, copies of the form returned to CBN/NFIU and the supporting documentation should be retained. Financial institutions are required to print search self-verification document and subject response list for documentation purpose.

The **Subject Response List** displays the total number of positive responses submitted to CBN/NFIU for that transmission, the transmission date, the submitted date, the tracking number and subject name that had the positive hit. If the financial institution

elects to maintain copies of such requests, the Examiner should not criticize it for doing so, **as long as it appropriately secures them and protects their confidentiality.** Audit reports should include an evaluation of compliance with these guidelines within their scope.

CBN/NFIU will regularly updates a list of search transmissions, including information on the date of transmission, tracking number and number of subjects listed in the transmission. Examiners may review this subject-list to verify that search requests have been received. Each financial institution should contact its primary regulator for guidance to ensure it obtains the subject-list and for updating contact information.

Voluntary Information Sharing

Financial institutions and their associates are encouraged to share information in order to identify and report activities that may involve terrorist activity or money laundering. Financial institutions should however notify the CBN/NFIU of its intent to engage in information sharing and that it has established and will maintain adequate procedures to protect the security and confidentiality of the information. Failure to comply with this requirement will result in loss of safe-harbour protection for information sharing and may result in a violation of privacy laws or other laws and regulations.

If a financial institution chooses to voluntarily participate in VIS, policies, procedures and processes should be developed and implemented for sharing and receiving of information.

Notice to share information given to CBN/NFIU

The financial institution should designate a point of contact for receiving and providing information. A financial institution should establish a process for sending and receiving information sharing requests. Additionally, a financial institution must take reasonable steps to verify that the other financial institution or association of financial institutions with which it intends to share information has also submitted the required notice to CBN/NFIU. The CBN/NFIU provides participating financial institutions with access to a list of other participating financial institutions and their related contact information.

If a financial institution receives such information from another financial institution, it must also limit the use of the information and maintain its security and confidentiality.

Such information may be used only to identify and render returns on money laundering and terrorist financing; to determine whether to establish or maintain an account; to engage in other forms of transactions; or to assist in complying with MLPA & AML/CFT Regulation.

The procedures to ensure confidentiality will be considered adequate if the financial institution applies procedures similar to the ones it has established to comply with the

regulation on the protection of its customers' non-public personal information. The VIS does not authorize a financial institution to share information on suspicious transactions, nor does it permit the financial institution to disclose the existence or non-existence of such transactions.

If financial institution shares information under VIS about the subject on STR, the information shared should be limited to underlying transaction and customer information. A financial institution may use information obtained under VIS to determine whether to file a STR, but the intention to prepare or file a STR cannot be shared with another financial institution. Financial institutions should establish a process for determining when and if a STR should be filed.

Actions taken pursuant to information obtained through the VIS process do not affect a financial institution's obligations to respond to any legal process. Additionally, actions taken in response to information obtained through the voluntary information sharing process do not relieve a financial institution of its obligation to file a STR and to immediately notify the LEA (if necessary) in accordance with all applicable laws and regulations.

9. OVERVIEW OF PURCHASE AND SALE OF MONETARY INSTRUMENTS RECORD-KEEPING

Purchaser Verification

Financial institutions are required to verify the identity of persons purchasing monetary instruments for cash in **tandem with the reportable threshold amount of N1 million & above or USA \$1,000**, and to maintain records of all such sales.

Financial institutions **should** either verify that the purchaser of monetary instruments is a deposit account holder with identifying information on record with the financial institution, or a financial institution may verify the identity of the purchaser in accordance with the form of identification contained in AML/CFT Regulation in respect of the customer's name and address and other means of identification acceptable by the financial community for cashing cheques by non-customers. The financial institution must obtain additional information for purchasers who do not have deposit accounts. The method used to verify the identity of the purchaser must be recorded.

Indirect Currency Purchases of Monetary Instruments

Financial institutions may implement a policy requiring customers who are deposit account holders and who want to purchase monetary instruments in amounts of **N1 million for individuals, N5 million for corporate entities or USA \$1,000** with cash to first deposit the cash into their deposit accounts. Nothing within the CBN AML/CFT Regulation 2009 or other regulations prohibits a financial institution from instituting such a policy.

However, when a customer purchases a monetary instrument in amounts of **N1 million for individuals, N5 million for corporate entities or USA \$1,000** using cash, the customer should first deposit such cash into his/its account, the transaction is still subject to the regulatory recordkeeping and reporting requirements. These requirements apply whether the transaction is conducted in accordance with a financial institution's established policy or at the request of the customer. Generally, when a bank/**other financial institution** sells monetary instruments to deposit account holders, it is expected to already maintain most of the regulatory required information in the normal course of its business.

Record keeping and Retention Requirements

A financial institution's records of sales must contain, at a minimum, the following information:

If the purchaser **has a deposit account** with the bank:

- i. Name of the purchaser.
- ii. Date of purchase.
- iii. Types of instruments purchased.
- iv. Serial numbers of each of the instruments purchased.
- v. Amounts of each of the instruments purchased in Naira or other currencies.
- vi. Specific identifying information, if applicable.

If the **purchaser does not have a deposit account** with the financial institution:

- i. Name and address of the purchaser.
- ii. Social security or alien identification number of the purchaser.
- iii. Date of birth of the purchaser.
- iv. Date of purchase.
- v. Types of instruments purchased.
- vi. Serial numbers of each of the instruments purchased.
- vii. Naira **or other currencies** amount of each of the instruments purchased.
- viii. Specific identifying information for verifying the purchaser's identity (e.g. state of issuance and number on driver's licence).

If the purchaser cannot provide the required information at the time of the transaction or through the financial institution's own previously verified records, **the transaction should be refused**. The records of monetary instrument sales must be retained for five years and be available for & reported to CBN, NFIU, auditors **and other** competent authorities.

10. OVERVIEW OF FUNDS TRANSFERS RECORD-KEEPING

Every financial institution is required to comply with statutory and regulatory requirements for funds transfers.

The regulatory requirements are set forth in the MLPA, 2004 and CBN AML/CFT Regulation, 2009.

Funds transfer systems enable instantaneous transfer of funds, including both domestic and cross-border transfers. Consequently these systems can present an attractive method to disguise the source of funds derived from illegal activity. The CBN AML/CFT Regulation, 2009 requires each financial institution involved in funds transfers to collect and retain certain information in connection with funds transfers of USA **\$1,000 or more**. The information required to be collected and retained depends on the financial institution's role in the particular funds transfer (originator's financial institution, intermediary financial institution, or beneficiary's financial institution). The requirements may also vary depending on whether an originator or beneficiary is an established customer of a financial institution and whether a payment order is made in person or otherwise.

It also requires all financial institutions to include certain information in transmittal orders for funds transfers of USA **\$1,000** or more.

Responsibilities of Originator's Financial Institutions Record-keeping Requirements

For each payment order in the amount of USA **\$1,000** or more that a financial institution accepts as an originator's financial institution, it must obtain and retain the following records:

- i. Name and address of the originator.
- ii. Amount of the payment order.
- iii. Date of the payment order.
- iv. Any payment instructions.
- v. Identity of the beneficiary's institution.
- vi. As many of the following items as are received with the payment order:
 - a. Name and address of the beneficiary.

- b. Account number of the beneficiary.
- c. Any other specific identifier of the beneficiary.

Additional Record-keeping Requirements for Non-established Customers

If the originator is not an established customer of the financial institution, the originator's financial institution must collect and retain the information listed above. In addition, the originator's financial institution must collect and retain other information, depending on whether the payment order is made in person by the originator.

Payment Orders Made in Person

If the payment order is made in person by the originator, the originator's financial institution must verify the identity of the person placing the payment order before it accepts the order. If it accepts the payment order, the originator's financial institution must obtain and retain the following records:

- i. Name and address of the person placing the order.
- ii. Type of identification document reviewed.
- iii. Number of the identification document (e.g., driver's licence).
- iv. The person's Taxpayer Identification Number (TIN) [e.g., National I.D. number or Employer Identification Number (EIN)] or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of lack of it thereof.

If the originator's financial institution has knowledge that the person placing the payment order is not the originator, the originator's financial institution must obtain and record the originator's TIN or, if none, the alien identification number or passport number and country of issuance, or a notation of lack of it thereof.

Payment Orders Not Made in Person

If a payment order is not made in person by the originator, the originator's financial institution must obtain and retain the following records:

- i. Name and address of the person placing the payment order.
- ii. The person's TIN or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of lack of it thereof, and a copy or record of the method of payment (e.g., cheque or credit card transaction) for the funds transfer.

If the originator's financial institution has knowledge that the person placing the payment order is not the originator, the originator's financial institution must obtain and

record the originator's TIN or, if none, the alien identification number or passport number and country of issuance, or a notation of lack of it thereof.

Irretrievability

Information retained must be **retrievable by reference to the name of the originator**. When the originator is an established customer of the financial institution and has an account used for funds transfers, information retained must also be **retrievable by account number**. Records must be maintained for five years.

Travel Rule Requirement

For funds transmittals of USA \$1,000 or more, the transmitter's financial institution must include the following information in the transmittal order at the time that a transmittal order is sent to a receiving financial institution:

- i. Name and account number of the transmitter, and, if the payment is ordered from an account.
- ii. Address of the transmitter.
- iii. Amount of the transmittal order.
- iv. Date of the transmittal order.
- v. Identity of the recipient's financial institution.
- vi. As many of the following items as are received with the transmittal order:
 - a. Name and address of the recipient.
 - b. Account number of the recipient.
 - c. Any other specific identifier of the recipient.
- vii. Either the name and address or the numerical identifier of the transmitter's financial institution.

Responsibilities of Intermediary Institutions

Recordkeeping Requirements

For each payment order of **USA \$1,000** or more that a financial institution accepts as an intermediary financial institution, the institution must retain a record of the payment order.

Travel Rule Requirements

For funds transmittals of USA \$1,000 or more, the intermediary financial institution must include the following information if received from the sender in a transmittal order at the time that order is sent to a receiving financial institution:

- i. Name and account number of the transmittor.
- ii. Address of the transmittor.
- iii. Amount of the transmittal order.
- iv. Date of the transmittal order.
- v. Identity of the recipient's financial institution.
- vi. As many of the following items as are received with the transmittal order:
 - a. Name and address of the recipient.
 - b. Account number of the recipient.
 - c. Any other specific identifier of the recipient.
- vii. Either the name and address or the numerical identifier of the transmittor's financial institution.

Intermediary financial institutions must pass on all the information received from a transmittor's financial institution or the preceding financial institution, but they have no duty to obtain information not provided by the transmittor's financial institution or the preceding financial institution.

Responsibilities of Beneficiary's Financial Institutions

Recordkeeping Requirements

For each payment order of USA \$1,000 or more that a financial institution accepts as a beneficiary's financial institution, the institution must retain a record of the payment order.

If the beneficiary is not an established customer of the financial institution, the beneficiary's institution must retain the above information for each payment order of USA \$1,000 or more.

Proceeds Delivered in Person

If proceeds are delivered in person to the beneficiary or its representative or agent, the institution must verify the identity of the person receiving the proceeds and retain a record of the following:

- i. Name and address.
- ii. The type of document reviewed.
- iii. The number of the identification document.

- iv. The person's TIN, or, if none, the alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof.
- v. If the institution has knowledge that the person receiving the proceeds is not the beneficiary, the institution must obtain and retain a record of the beneficiary's name and address, as well as the beneficiary's identification.

Proceeds Not Delivered in Person

If proceeds are not delivered in person, the institution must retain a copy of the cheque or other instrument used to effect the payment, or the institution must record the information on the instrument. The institution must also record the name and address of the person to whom it was sent.

Irretrievability

Information retained must be retrievable by reference to the name of the beneficiary. When the beneficiary is an established customer of the institution and has an account used for funds transfers, information retained must also be retrievable by account number.

There are **no Travel Rule requirements** for beneficiary financial institutions.

Abbreviations and Addresses

Although the use of coded names or pseudonyms are not permitted, the use of abbreviated names, names reflecting different accounts of a corporation (e.g., XYZ Payroll Account), and trade and assumed names of a business ("doing business as") or the names of unincorporated divisions or departments of the business are allowed.

Customer Address

Customer's street address is required to be included in a transmittal order and this should be known to the transmitter's financial institution.

The regulatory interpretation of the term "address" means either the transmitter's street address or the transmitter's address maintained in the financial institution's automated CIF (not mailing address such as post office box) as long as the institution maintains the transmitter's address on file and the address information is retrievable upon request by LEA.

Certifications

A financial institution that maintains a correspondent account for a foreign financial institution must **maintain records identifying the owners of each foreign**

financial institution. A financial institution must also record the name and street address of a person who resides in Nigeria and who is authorized, and has agreed, to be an agent to accept service of legal process. A financial institution must produce these records within seven days upon receipt of a written request from a LEA.

Account Closure

Financial institutions must obtain certifications (or re-certifications) or the required information within 30 calendar days after the date an account is established and at least once every three years thereafter. If the financial institution is unable to obtain the required information, it must close all correspondent accounts with the foreign financial institution within a commercially reasonable time.

Verification

A financial institution should review certifications for reasonableness and accuracy. If a financial institution at any time knows, suspects, or has reason to suspect that any information obtained or that any other information it relied on is no longer correct, the financial institution must request the foreign financial institution to verify or correct such information, or the financial institution must take other appropriate measures to ascertain its accuracy. Therefore, financial institutions should review certifications for potential problems that may warrant further review, such as use of post office boxes or forwarding addresses.

If the financial institution has not obtained the necessary or corrected information within 90 days, it must close the account within a commercially reasonable time. During this time, the financial institution may not permit the foreign financial institution to establish any new financial positions or execute any transactions through the account, other than those transactions necessary to close the account. Also, a financial institution may not establish any other correspondent account for the foreign financial institution until it obtains the required information.

A financial institution must also retain the original of any document provided by a foreign financial institution, and retain the original or a copy of any document otherwise relied on for the purposes of the regulation, for at least five years after the date that the financial institution no longer maintains any correspondent account for the foreign financial institution.

Requests for AML Records by Regulator

Also, upon request by its regulator(s), a financial institution must provide or make available records related to its AML compliance or one of its customers within three (3) working days from the time of the request.

Special Due Diligence Program for Foreign Correspondent Accounts

This subsection requires each financial institution that establishes, maintains, administers, or manages a correspondent account for a foreign financial institution to take certain AML measures for such accounts.

General Due Diligence

Financial institutions are required to establish a due diligence program that includes appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures and controls that are reasonably designed to enable the financial institution to detect and report, on an ongoing basis, any known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed by it for a foreign financial institution.

Due diligence policies, procedures and controls must include each of the following:

- i. Determining whether each such foreign correspondent account is subject to "Enhanced Due Diligence" (EDD).
- ii. Assessing the money laundering risks presented by each such foreign correspondent account.
- iii. Applying risk-based procedures and controls to each such foreign correspondent account reasonably designed to detect and report known or suspected money laundering activity, including a periodic review of the correspondent account activity sufficient to determine consistency with information obtained about the type, purpose and anticipated activity of the account.

Risk assessment of foreign financial institutions

A financial institution's general due diligence program must include policies, procedures and processes to assess the risks posed by its foreign financial institution customers. A financial institution's resources are most appropriately directed at those accounts that pose a more significant money laundering risk. Its due diligence program should provide for the risk assessment of foreign correspondent accounts considering all relevant factors, including, as appropriate:

- i. The nature of the foreign financial institution's business and the markets it serves.
- ii. The type, purpose and anticipated activity of the foreign correspondent account.
- iii. The nature and duration of the financial institution's relationship with the foreign financial institution (and, if relevant, with any affiliate of the foreign financial institution).
- iv. The AML and supervisory regime of the jurisdiction that issued the charter or licence to the foreign financial institution and, to the extent that information regarding such jurisdiction is reasonably available, of the jurisdiction in which any company that is an owner of the foreign financial institution is incorporated or chartered.
- v. Information known or reasonably available to the financial institution about the foreign financial institution's AML record, including public information in standard industry guides, periodicals and major publications.

Monitoring of foreign correspondent accounts

As part of ongoing due diligence, financial institutions should periodically review their foreign correspondent accounts. Monitoring will not, in the ordinary situation, involve scrutiny of every transaction taking place within the account, but, instead, should involve a review of the account sufficient to ensure that the financial institution can determine whether the nature and volume of account activity are generally consistent with information regarding the purpose of the account and expected account activity and to ensure that the financial institution can adequately identify suspicious transactions.

An effective due diligence program will provide for a range of due diligence measures, based upon the financial institution's risk assessment of each foreign correspondent account. The starting point for an effective due diligence program, therefore, should be a stratification of the money laundering risk of each foreign correspondent account based on the financial institution's review of relevant risk factors (such as those identified above) to determine which accounts may require increased measures. The due diligence program should identify risk factors that would warrant the institution conducting additional scrutiny or increased monitoring of a particular account. As due diligence is an ongoing process, a financial institution should take measures to ensure account profiles are current and monitoring should be risk-based. Financial institutions should consider whether risk profiles should be adjusted or suspicious activity reported when the activity is inconsistent with the profile.

Enhanced Due Diligence

Financial institutions are required to establish risk-based EDD policies, procedures and controls when establishing, maintaining, administering or managing a correspondent account in Nigeria for foreign financial institutions operating under any one or more of the following:

- i. An **offshore banking licence**.
- ii. A **banking licence issued by a foreign country** that has been designated as non-cooperative with international AML principles or procedures by an inter-governmental group or organization of which Nigeria is a member and Nigeria representative to the group or organization concurs its decision.
- iii. A **banking licence issued by a foreign country that has been designated by the CBN as warranting special measures** due to money laundering concerns.

If such an account is established or maintained, the financial institution is required to establish EDD policies, procedures and controls to ensure that it, at a minimum, takes reasonable steps to:

- i. Determine, for any such foreign financial institution whose shares are not publicly traded, the identity of each of the owners of the foreign financial institution and the nature and extent of the ownership interest of each such owner;
- ii. Conduct enhanced scrutiny of such account to guard against money laundering and to identify and report any suspicious transactions in accordance with applicable laws and regulations. This enhanced scrutiny is to reflect the risk assessment of the account and shall include, as appropriate;
- iii. Obtain and consider information relating to the foreign financial institution's anti-money laundering program to assess the risk of money laundering presented by the foreign financial institution's correspondent account;
- iv. Monitor transactions to, from, or through the correspondent account in a manner reasonably designed to detect money laundering and suspicious activity;
- v. Obtain information from the foreign financial institution about the identity of any person with authority to direct transactions through any correspondent account that is a payable through account, and the sources and the beneficial owner of funds or other assets in the payable through account; and
- vi. Determine whether the foreign financial institution for which the correspondent account is maintained in turn maintains correspondent accounts for other foreign financial institutions that use the foreign financial institution's correspondent account. If so, take reasonable steps to obtain information relevant to assess and mitigate money laundering risks associated with the foreign financial institution's correspondent accounts for

other foreign financial institutions, including, as appropriate, the identity of those foreign financial institutions.

In addition to those categories of foreign financial institutions identified in the regulation as requiring EDD, financial institutions may find it appropriate to conduct additional due diligence measures on foreign financial institutions identified through application of the financial institution's general due diligence program as posing a higher risk for money laundering. Such measures may include any or all of the elements of EDD set forth in the regulation, as appropriate for the risks posed by the specific foreign correspondent account.

As also noted in the above section on general due diligence, a financial institution's resources are most appropriately directed at those accounts that pose a more significant money laundering risk. Accordingly, where a financial institution is required or otherwise determines that it is necessary to conduct EDD in connection with a foreign correspondent account, the financial institution may consider the risk assessment factors discussed in the section on general due diligence when determining the extent of the EDD that is necessary and appropriate to mitigate the risks presented. In particular, the anti-money laundering and supervisory regime of the jurisdiction that issued a charter or licence to the foreign financial institution may be especially relevant in a financial institution's determination of the nature and extent of the risks posed by a foreign correspondent account and the extent of the EDD to be applied.

Special Procedures When Due Diligence Cannot Be Performed

A financial institution's due diligence policies, procedures and controls established **must include procedures to be followed in circumstances when appropriate due diligence or EDD cannot be performed** with respect to a foreign correspondent account and when the financial institution should:

- i. Refuse to open the account
- ii. Suspend transaction activity
- iii. File STR
- iv. Close account

11. OVERVIEW OF PRIVATE BANKING DUE DILIGENCE PROGRAM (NON-NIGERIANS)

Financial institutions are required to comply with the statutory and regulatory requirements by implementing policies, procedures and controls to detect and report money laundering and suspicious activity through private banking accounts established, administered or maintained for non-Nigerian persons.

Private banking can be broadly defined as providing personalized financial services to wealthy clients. In particular, a financial institution must establish appropriate, specific and (where necessary) EDD policies, procedures and controls that are reasonably designed to enable the financial institution to detect and report instances of money laundering through such accounts.

CBN AML/CFT Regulation, 2009 mandates enhanced scrutiny to detect and, if appropriate, report transactions that may involve proceeds of foreign corruption for private banking accounts that are requested or maintained by or on behalf of a senior foreign/local political figure or the individual's immediate family and close associates.

Private Banking Accounts

A "private banking account" is an account (or any combination of accounts) either so-called private bank account or maintained at a financial institution that satisfies all the three criteria:

1. Requires a minimum aggregate deposit of funds or other assets of not less than USA \$50,000 or its equivalent;
2. Is established on behalf of or for the benefit of one or more Nigerian or non-Nigerian persons who are direct or beneficial owners of the account; and
3. Is assigned to, or is administered by, in whole or in part, an officer, employee, or agent of a financial institution acting as a liaison between a financial institution covered by the regulation and the direct or beneficial owner of the account.

With regard to the minimum deposit requirement, a "private banking account" is an account (or combination of accounts) that requires a minimum deposit of not less than USA \$50,000 or its equivalent. A financial institution may offer a wide range of services that are generically termed private banking, and even if certain (or any combination, or all) of the financial institution's private banking services do not require a minimum deposit of not less than USA \$50,000 or its equivalent, **these relationships should be subject to a greater level of due diligence under the financial institution's risk-based AML compliance program.**

Due Diligence Program

A financial institution is required to establish and maintain a due diligence program that includes policies, procedures and controls that are reasonably designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving any private banking account for a Nigerian or non-Nigerian person

that is established, maintained, administered, or managed in the Nigeria by the financial institution. **The due diligence program must ensure that, at a minimum, the financial institution takes reasonable steps to do each of the following:**

- i. Ascertain the identity of all nominal and beneficial owners of a private banking account.
- ii. Ascertain whether the nominal or beneficial owner of any private banking account is a senior local/foreign political figure.
- iii. Ascertain the source(s) of funds deposited into a private banking account and the purpose and expected use of the account.
- iv. Review the activity of the account to ensure that it is consistent with the information obtained about the client's source of funds, and with the stated purpose and expected use of the account, and to file a STR, as appropriate, to report any known or suspected money laundering or suspicious activity conducted to, from, or through a private banking account.

Risk Assessment of Private Banking Accounts for Nigerian/Non-Nigerian Persons

The nature and extent of due diligence conducted on private banking accounts for Nigerian/non- Nigerian persons will likely vary for each client depending on the presence of potential risk factors. More extensive due diligence, for example, may be appropriate for new clients; clients who operate in, or whose funds are transmitted from or through jurisdictions with weak AML controls; and clients whose lines of business are primarily currency-based (e.g., casinos or currency exchangers). Due diligence should also be commensurate with the size of the account. Accounts with relatively more deposits and assets should be subject to greater due diligence. In addition, if the financial institution at any time learns of information that casts doubt on previous information, further due diligence would be appropriate.

Ascertaining Source of Funds and Monitoring Account Activity

Financial institutions that provide private banking services generally are required to obtain considerable information about their clients, including the purpose for which the customer establishes the private banking account. This information can establish a baseline for account activity that will enable a financial institution to better detect suspicious activity and to assess situations where additional verification regarding the source of funds may be necessary. Financial institutions are not expected, in the ordinary course of business, to verify the source of every deposit placed into every private banking account. However, financial institutions should monitor deposits and transactions as necessary to ensure that activity is consistent with information that the financial institution has received about the client's source of funds and with the stated

purpose and expected use of the account. Such monitoring will facilitate the identification of accounts that warrant additional scrutiny.

Enhanced Scrutiny of Private Banking Accounts for Senior Local/Foreign Political Figures

The term “senior political figure” is defined to include one or more of the following:

- i. A current or former Senior official in the executive, legislative, administrative, military, or judicial branches of a foreign government (whether elected or not).
- ii. Senior official of a major foreign political party.
- iii. Senior executive of a foreign-government-owned commercial enterprise.
- iv. A corporation, business, or other entity that has been formed by, or for the benefit of, any such individual.
- v. An immediate family member (including spouses, parents, siblings, children, and a spouse’s parents and siblings) of any such individual.
- vi. A person who is widely and publicly known (or is actually known by the relevant financial institution) to be a close associate of such individual.

Senior political figures as defined above are often referred to as “Politically Exposed Persons” or PEPs. For private banking accounts for which a senior local/foreign political figure is a nominal or beneficial owner, the financial institution’s due diligence program must include enhanced scrutiny that is reasonably designed to detect and report transactions that may involve the proceeds of local/foreign corruption. The term “proceeds of local/foreign corruption” means any asset or property that is acquired by, through, or on behalf of a senior local/foreign political figure through misappropriation, theft, or embezzlement of public funds, the unlawful conversion of property of a foreign government, or through acts of bribery or extortion, and includes any other property into which any such assets have been transformed or converted.

Enhanced scrutiny of private banking accounts for senior local/foreign political figures should be risk-based. Reasonable steps to perform enhanced scrutiny may include consulting publicly available information regarding the home country of the client, contacting branches of the financial institution operating in the home country of the client to obtain additional information about the client and the political environment, and conducting greater scrutiny of the client’s employment history and sources of income. For example, funds transfers from a government account to the personal account of a government official with signature authority over the government account may raise a financial institution’s suspicions of possible political corruption. In addition, if a financial institution’s review of major news sources indicates that a client may be or is involved in political corruption, the financial institution should review the client’s account for unusual activity and:

- i. Refuse to open the account.
- ii. Suspend transaction activity.
- iii. File an STR.
- iv. Close the account.

Identifying Senior Political Figures

Financial institutions are required to establish policies, procedures and controls that include reasonable steps to ascertain the status of an individual as a senior political figure. Procedures should require obtaining information regarding employment and other sources of income, and the financial institution should seek information directly from the client regarding possible senior local/foreign political figure status. The financial institution should also check references, as appropriate, to determine whether the individual holds or has previously held a senior political position or may be a close associate of a senior local/foreign political figure. In addition, the financial institution should make reasonable efforts to review public sources of information regarding the client.

Financial institutions applying reasonable due diligence procedures in accordance with regulatory requirements may not be able to identify, in every case, individuals who qualify as senior local/foreign political figures, and, in particular, their close associates, and thus may not apply enhanced scrutiny to all such accounts. If the financial institution's due diligence program is reasonably designed to make this determination, and it administers this program effectively, then the financial institution should generally be able to detect, report and take appropriate action when suspected money laundering is occurring with respect to these accounts, even in cases when the financial institution has not been able to identify the accountholder as a senior foreign political figure warranting enhanced scrutiny.

Special Procedures When Due Diligence Cannot Be Performed

A financial institution's due diligence policies, procedures and controls established must include special procedures when appropriate due diligence cannot be performed. **These special procedures must include when the financial institution should:**

- i. Refuse to open the account.
- ii. Suspend transaction activity.
- iii. File an STR.
- iv. Close the account.

12. OVERVIEW OF SPECIAL MEASURES

Financial institutions and domestic financial agencies are required to take certain special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern.

Types of Special Measures

They are to take following special measures either individually, jointly or in any combination:

Record keeping and Reporting of Certain Financial Transactions

Under the first special measure, financial institutions are required to maintain records or file reports or both, concerning the aggregate amount of transactions or the specifics of each transaction with respect to a jurisdiction, financial institution, class of transactions or type of account that is of primary money laundering concern.

Information Relating to Beneficial Ownership

Under the second special measure, financial institutions are required to take reasonable and practicable steps to obtain and retain information concerning the beneficial ownership of any account opened or maintained by a foreign person (other than a foreign entity whose shares are subject to public reporting requirements or are listed and traded on a regulated exchange or trading market), or a representative of such foreign person that involves a jurisdiction, financial institution, class of transactions or type of account that is of primary money laundering concern.

Information Relating to Certain Payable through Accounts

Under the third special measure, financial institutions that open or maintain a payable through account involving a jurisdiction, financial institution, class of transactions or type of account **that is of primary money laundering concern** are required:

- i. To identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account; and
- ii. To obtain information about each customer (and representative) that is substantially comparable to that which the financial institution obtains in the ordinary course of business with respect to its customers residing in Nigeria.

Information Relating to Certain Correspondent Accounts

Under the fourth special measure, financial institutions that open or maintain a correspondent account involving a jurisdiction, financial institution, class of transactions or type of account **that is of primary money laundering concern** are required to:

- i. Identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account; and
- ii. Obtain information about each such customer (and representative) that is substantially comparable to that which a depository institution obtains in the ordinary course of business with respect to its customers residing in Nigeria.

13. OVERVIEW OF INTERNATIONAL TRANSPORTATION OF CURRENCY OR MONETARY INSTRUMENTS REPORTING

Financial institutions are required to comply with statutory and regulatory requirements for the reporting of international shipments of currency or monetary instruments.

Each person (including a financial institution) who physically transports, mails or ships currency or monetary instruments in excess of USA **\$10,000** at one time out of or into Nigeria (and each person who causes such transportation, mailing or shipment) **must file a Declaration Report with the Nigeria Customs Services (NCS) at the time of entry into or departure from Nigeria.**

When a person receives currency or monetary instruments through financial institution in an amount exceeding USA **\$10,000** at one time that have been shipped from any place outside Nigeria, a report must be filed with NCS within 15 days of receipt of the instruments (unless a report has already been filed). The report is to be completed by or on behalf of the person requesting transfer of the currency or monetary instruments.

Financial institutions are also required to report these items if they are mailed or shipped through the postal service or by common carrier. However, a financial institution or trust company recognized under the law is not required to report overland shipments of currency or monetary instruments if they are shipped to or received from an established customer maintaining a deposit relationship with the financial institution where the latter can reasonably conclude that the amounts do not exceed what is commensurate with the customary conduct of the business, industry or profession of the customer concerned.

Management should implement applicable policies, procedures and processes for filing these declaration reports. Management should review the international transportation of currency and monetary instruments.

Monitoring Of Office of Foreign Assets Control (OFAC) List

Financial institutions are required to establish procedures and processes of monitoring and identifying OFAC blocked countries, entities, etc. Also assess the appropriateness of the procedures and processes are also to be appropriate, taking into consideration the financial institution's products, services, customers, entities, transactions, geographical locations and its scope of international operations.

Though complying with OFAC requirements is mandatory to only U.S. based banks, it is important that financial institutions in Nigeria be aware of these requirements and take notice of all OFAC blocked/banned countries, terrorists, entities, etc. This would enable the financial institutions know and avoid carrying out transactions with blocked entities as transactions that pass through a U.S. correspondent bank would be confiscated. This could cause both financial and reputation loss to the Nigerian financial institution victims.

Financial institutions are therefore required to have procedures and processes of knowing the requirements, updating them, monitoring and reporting transactions with entities, countries, etc on the OFAC List.

OFAC Reporting

Financial institutions are required to report all blockings to CBN and NFIU within 10 days of the occurrence and annually by December 31 concerning those assets blocked. Once assets or funds are blocked, they should be placed in a blocked account. Prohibited transactions that are rejected must also be reported to CBN and NFIU within 10 days of the occurrence.

Financial institutions are required to also keep a full and accurate record of each rejected transaction for at least five years after the date of the transaction. For blocked property (including blocked transactions), records must be maintained for the period the property is blocked and for five years after the date the property is unblocked. Officers are requested to obtain additional information concerning OFAC regulations, such as Sanctions Program and Country Summaries Brochures; the **Specially Designated Nationals (SDN) or Blocked Persons List** (including both entities and individuals); recent OFAC actions; and "Frequently Asked Questions," from OFAC's Web site.

OFAC Compliance Program

As a matter of sound banking practice and in order to ensure compliance, financial institutions should establish and maintain an effective written OFAC compliance program commensurate with their OFAC risk profile based on products, services, customers, and geographic locations. The program should identify higher-risk areas, provide for appropriate internal controls for screening and reporting, establish

independent testing for compliance, designate the institution's employee or employees as responsible for OFAC compliance and create adequate training programs for appropriate officers.

OFAC Risk Assessment

A fundamental element of a sound OFAC compliance program is the institution's assessment of its specific product lines, customer base and nature of transactions and identification of higher-risk areas for OFAC transactions. The initial identification of higher-risk customers for purposes of OFAC may be performed as part of the bank's CIP and CDD procedures. As OFAC sanctions can reach into virtually all areas of operations, financial institutions should consider all types of transactions, products and services when conducting their risk assessment and establishing appropriate policies, procedures and processes.

An effective risk assessment should be a composite of multiple factors. It depends upon the circumstances and certain factors may be weighed more heavily than others.

Another consideration for the risk assessment is the account and transaction parties. New accounts should be compared with OFAC lists prior to being opened or shortly thereafter. However, the extent to which the institution includes account parties other than accountholders (e.g., beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories and powers of attorney) in the initial OFAC review during the account opening process, and during subsequent database reviews of existing accounts, will depend on the institution's risk profile and available technology.

Based on the institution's OFAC risk profile for each area and available technology, it should establish policies, procedures and processes for reviewing transactions and transaction parties (e.g., issuing bank, payee, endorser and jurisdiction). In evaluating the level of risk, the institution should exercise judgment and take into account all indicators of risk. **Although not an exhaustive list, examples of products, services, customers and geographic locations that may carry a higher level of OFAC risk include:**

- i. International funds transfers.
- ii. Nonresident alien accounts.
- iii. Foreign customer accounts.
- iv. Cross-border automated clearing house (ACH) transactions.
- v. Commercial letters of credit and other trade finance products.
- vi. Transactional electronic banking.
- vii. Foreign correspondent bank accounts.
- viii. Payable through accounts.
- ix. International private banking.

- x. Overseas branches or subsidiaries.

Internal Controls

An effective OFAC compliance program should include internal controls for identifying suspect accounts and transactions and reporting to OFAC. **Internal controls should include the following elements:**

i. Identifying and reviewing suspicious transactions

The institution's policies, procedures and processes should address how it will identify and review transactions and accounts for possible OFAC violations, whether conducted manually, through interdiction software or a combination of both. For screening purposes, the institution should clearly define its criteria for comparing names provided on the OFAC list with the names in its files or on transactions and for identifying transactions or accounts involving sanctioned countries. The policies, procedures and processes should also address how it will determine whether an initial OFAC hit is a valid match or a false hit.

A high volume of false hits may indicate a need to review the institution's interdiction program. The screening criteria used by financial institutions to identify name variations and misspellings should be based on the level of OFAC risk associated with the particular product or type of transaction. For example, in a higher-risk area with a high-volume of transactions, the institution's interdiction software should be able to identify close name derivations for review. The Specially Designated Nationals (SDN)/Blocked Persons List's attempts to provide name derivations may not include all derivations. More sophisticated interdiction software may be able to catch variations of an SDN's name not included on the SDN list.

Lower-risk institutions or areas and those with low volumes of transactions may decide to manually filter for OFAC compliance. Decisions to use interdiction software and the degree of sensitivity of that software should be based on an institution's assessment of its risk and the volume of its transactions. In determining the frequency of OFAC checks and the filtering criteria used (e.g., name derivations), financial institutions should consider the likelihood of incurring a violation. In addition, financial institutions should periodically reassess their OFAC filtering system. For example, if an institution identifies a name derivation of an OFAC target, OFAC guidelines suggest that the institution adds the name to its filtering process.

New accounts should be compared with the OFAC lists prior to being opened or shortly thereafter. Financial institutions that perform OFAC checks after account opening should have procedures in place to prevent transactions, other than initial deposits from occurring until the OFAC check is completed. Prohibited transactions conducted prior to

completing an OFAC check are subject to penalty action. In addition, financial institutions are required to have policies, procedures and processes in place to check existing customers when there are additions or changes to the OFAC list.

The frequency of the review should be based on the institution's OFAC risk.

For example, institutions with a lower OFAC risk level may periodically (e.g., monthly or quarterly) compare the customer base against the OFAC list. Transactions such as funds transfers, letters of credit and noncustomer transactions should be checked against OFAC lists prior to being executed. When developing OFAC policies, procedures and processes, the institution should keep in mind that the continued operation of an account or the processing of transactions post-designation, along with the adequacy of their OFAC compliance program will be a factor in determining penalty actions to be imposed. **The institution should maintain documentation of its OFAC checks on new accounts, the existing customer base and specific transactions.**

If an institution uses a third party, such as an agent or service provider, to perform OFAC checks on its behalf, as with any other responsibility performed by a third party, it is ultimately responsible for that third party's compliance with the OFAC requirements. As a result, financial institutions should establish adequate controls and review procedures for such relationships.

ii. **Updating OFAC lists**

An institution's OFAC compliance program should include policies, procedures and processes for timely updating of the lists of blocked countries, entities and individuals and disseminating such information throughout its domestic operations and its offshore offices, branches and foreign subsidiaries. This would include ensuring that any manual updates of interdiction software are completed in a timely manner.

iii. **Reporting**

An OFAC compliance program should also include policies, procedures and processes for handling items that are validly blocked or rejected items under the various sanctions programs. In the case of interdictions related to narcotics trafficking or terrorism, financial institutions are required to notify CBN & NFIU as soon as possible by phone about potential hits with a follow-up in writing within ten days. Most other items should be reported through usual channels within ten days of the occurrence.

The policies, procedures and processes should also address the management of blocked accounts. Financial institutions are responsible for tracking the amount of blocked funds, the ownership of those funds and interest paid on those funds. Total amounts blocked, including interest must be reported to the CBN & NFIU by December 31 & June 30 of each year. When an institution acquires or merges with another, both institutions should take into consideration the need to review and maintain such records and

information. Financial institutions are required to also file STRs on blocked narcotics- or terrorism-related transactions in addition to the blocking reports rendered on OFAC.

iv. Maintaining licence information

Financial institutions are required to maintain copies of customers' OFAC licences in their files. This will allow the institution to verify whether or not a customer is initiating a legal transaction. institutions should also be aware of the expiration date on the licence. If it is unclear whether a particular transaction is authorized by a licence, the institution should confirm with OFAC. Maintaining copies of licences will also be useful if another institution in the payment chain requests verification of a licence's validity. Copies of licences should be maintained for five years, following the most recent transaction conducted in accordance with the licence.

v. Independent Testing

Every institution should conduct an independent test of its OFAC compliance program that is performed by the internal audit department, outside auditors, consultants or other qualified independent parties. For large institutions, the frequency and area of the independent test should be based on the known or perceived risk of specific business areas. For smaller institutions, the audit should be consistent with their OFAC risk profile or be based on a perceived risk. The person(s) responsible for testing should conduct an objective, comprehensive evaluation of OFAC policies, procedures and processes. The audit scope should be comprehensive enough to assess OFAC compliance risks and evaluate the adequacy of the OFAC compliance program.

vi. Responsible Individual

Every financial institution is required to designate a qualified individual(s) to be responsible for the day-to-day compliance of the OFAC compliance program, including the reporting of blocked or rejected transactions to the CBN & NFIU and the oversight of blocked funds. This individual should have an appropriate level of knowledge about OFAC regulations commensurate with the institution's OFAC risk profile.

vii. Training

The institution should provide adequate training for all appropriate employees. The scope and frequency of the training should be consistent with its OFAC risk profile and appropriate to employee responsibilities.

14. OVERVIEW AND PROCEDURES FOR CONSOLIDATED AND OTHER TYPES OF AML/CFT COMPLIANCE PROGRAM STRUCTURES

1. OVERVIEW OF AML/CFT COMPLIANCE PROGRAM STRUCTURES

A financial institution is required to ensure that its structure and management of its institution's AML/CFT Compliance Program and (if applicable) its consolidated or partially consolidated approach to AML/CFT are adequate.

Every financial institution is required to have a comprehensive AML/CFT Compliance Program that addresses the requirements of the Money Laundering (Prohibition) Act and CBN AML/CFT Regulation 2009 applicable to all its operations.

Each financial institution has discretion as to how its AML/CFT Compliance Program is structured and managed. It may structure and manage its AML/CFT Compliance Program or some parts of the program within a legal entity; with some degree of consolidation across entities within the institution; or as part of a comprehensive enterprise risk management framework.

Many large, complex financial institutions aggregate risk of all types (e.g., compliance, operational, credit, interest rate risk, etc.) on an institution-wide basis in order to maximize efficiencies and better identify, monitor and control all types of risks within or across affiliates, subsidiaries, lines of business or jurisdictions. In such institutions, management of MLPA, CBN AML/CFT Regulation 2009 risk is generally the responsibility of a corporate compliance function that supports and oversees the AML/CFT Compliance Program.

Other financial institutions may adopt a structure that is less centralized but still consolidates some or all aspects of AML/CFT compliance. For example, risk assessment, internal controls, suspicious transaction monitoring, independent testing or training may be managed centrally. Such centralization can effectively maximize efficiencies and enhance assessment of risks and implementation of controls across business lines, legal entities and jurisdiction of operation. For example, a centralized AML/CFT risk assessment function may enable a financial institution to determine its overall risk exposure to a customer doing business with it in multiple business lines or jurisdiction. Regardless of how a consolidated AML/CFT Compliance Program is organized, it should reflect the institution's business structure, size and complexity. It should be designed to effectively address risks, exposures and applicable legal requirements across the institution.

A consolidated approach should also include the establishment of corporate standards for AML/CFT compliance that reflect the expectations of the financial institution's board of directors, with senior management working to ensure that the Chief Compliance Officer implements these corporate standards. Individual lines of business policies would then supplement the corporate standards and address specific risks within the line of business or department.

A consolidated AML/CFT Compliance Program typically includes a central point where its risks throughout the institution are aggregated. Under a consolidated approach, risk should be assessed both within and across all business lines, legal entities and jurisdictions of operation. **Compliance Programs for global institutions should incorporate the AML laws and requirements of the various jurisdictions in which they operate.** Internal audit should assess the level of compliance with the consolidated AML/CFT Compliance Program.

Bank Examiners should be aware that some complex and diversified financial institutions may have various subsidiaries that hold different types of licences and banking charters or may organize business activities and AML/CFT Compliance Program components across their legal entities. For instance, a highly diversified financial institution may establish or maintain accounts using multiple legal entities that are examined by multiple regulators. This action may be taken in order to maximize efficiencies, enhance tax benefits, adhere to jurisdictional regulations, etc. This methodology may present a challenge to the Bank Examiner reviewing AML/CFT compliance in a legal entity within an institution. As appropriate, Examiners should coordinate efforts with other regulatory agencies in order to address these challenges or ensure the examination scope appropriately covers the legal entity examined.

Structure of the AML/CFT Compliance Function

Financial institution has discretion as how to structure and manage its AML/CFT Compliance Program. For example, a small institution may choose to combine its compliance with other functions and utilize the same personnel in several roles. In such circumstances, **there should still be adequate senior-level attention to AML/CFT compliance and sufficient dedicated resources. As is the case in all structures, the audit function should remain independent.**

A larger and more complex institution may establish a corporate AML/CFT compliance function to coordinate some or all its responsibilities. **For example, when there is delegation of AML/CFT compliance responsibilities and its Chief Compliance Officer is located within lines of business, expectations should be clearly set forth in order to avoid conflicts and ensure effective implementation of the AML/CFT Compliance Program.** In particular, allocation of responsibility should be clear with respect to the content and comprehensiveness of MIS reports, the depth and

frequency of monitoring efforts, and the role of different parties within the financial institution (e.g., risk, business lines, operations) in AML/CFT compliance decision-making processes. **A clear communication of which functions have been delegated and which remain centralized help to ensure consistent implementation of the AML/CFT Compliance Program among lines of business, affiliates and jurisdictions.** In addition, a clear line of responsibility may help to avoid conflicts of interest and ensure that objectivity is maintained.

Regardless of the management structure or size of the institution, AML/CFT compliance staff located within lines of business are not precluded from close interaction with the management and staff of the various business lines. AML/CFT compliance functions are often most effective when strong working relationships exist between compliance and business line staff.

In some compliance structures, the compliance officers could report to the management of the business line. This can occur in smaller institutions when the AML/CFT compliance officer reports to a senior officer; in larger institutions, the compliance officer could report to a line business manager; or in a foreign owned financial institution, its Nigeria's operations could be reported by the compliance officer to a single officer or executive. **These situations can present risks of potential conflicts of interest that could hinder effective AML/CFT compliance.**

To ensure the strength of compliance controls, an appropriate level of its compliance independence should be maintained, for example, by:

- i. Providing AML/CFT compliance officer a reporting line to the corporate compliance or other independent function;
- ii. Ensuring that AML/CFT compliance officer is actively involved in all matters affecting AML risk (e.g., new products, review or termination of customer relationships, filing determinations);
- iii. Establishing a process for escalating and objectively resolving disputes between AML/CFT compliance officer and business line management; and
- iv. Establishing internal controls to ensure that compliance objectivity is maintained when AML/CFT compliance officer is assigned additional responsibilities.

Management and Oversight of the AML/CFT Compliance Program

The board of directors and senior management of a financial institution have different responsibilities and roles in overseeing and managing AML/CFT compliance risk. The board of directors has primary responsibility for ensuring that the financial institution has a comprehensive and effective AMLCFT Compliance Program and oversight framework that is reasonably designed to ensure compliance with MLPA, AML/CFT

Regulation and related regulations. Senior management is responsible for implementing the board-approved AML/CFT Compliance Program.

Board of Directors

The board of directors is responsible for approving the AML/CFT Compliance Program and for overseeing the structure and management of its compliance function. The board is responsible for setting an appropriate culture of AML/CFT compliance, establishing clear policies regarding the management of key AML/CFT risks and ensuring that these policies are adhered to in practice.

The board should ensure that senior management is fully capable, qualified and properly motivated to manage the AML/CFT compliance risks arising from the institution's business activities in a manner that is consistent with the board's expectations. The board should ensure that its compliance function has an appropriately prominent status within the organization. Senior management within the AML/CFT compliance function and senior compliance personnel within the individual business lines should have the appropriate authority, independence and access to personnel and information within the organization and appropriate resources to conduct their activities effectively.

The board should ensure that its views about the importance of AML/CFT compliance are understood and communicated across all levels of the financial institution. The board also should ensure that senior management has established appropriate incentives to integrate AML/CFT compliance objectives into management goals and compensation structure across the organization, and that corrective actions, including disciplinary measures, if appropriate, are taken when serious AML/CFT compliance failures are identified.

Senior Management

Senior management is responsible for communicating and reinforcing the AML/CFT compliance culture established by the board, and implementing and enforcing the board-approved AML/CFT Compliance Program. If the financial institution has a separate AML/CFT compliance function, the senior management is required to establish, support and oversee the institution's AML/CFT Compliance Program. **AML/CFT chief compliance officer should report to the board or a committee thereof on effectiveness of the AML/CFT, Compliance Program and significant AML/CFT compliance matters.**

Senior management of a foreign owned financial institution is required to provide sufficient AML/CFT compliance information relating to its Nigerian operations to the board/senior management and control unit in its home country. It should also ensure

that responsible senior management in the home country has an appropriate understanding of the Nigerian AML/CFT risk and control environment governing its Nigeria operations. The management of such Nigerian financial institution should assess the effectiveness of established AML/CFT control mechanisms for Nigerian operations on an on-going basis, report and escalate areas of concern as needed. As appropriate, corrective action then should be developed and implemented.

Consolidated AML/CFT Compliance Programs

Financial institutions that centrally manage the operations and functions of their subsidiary financial institutions, other subsidiaries and business lines should ensure **that comprehensive risk management policies, procedures and processes are in place across the organization to address the entire organization's spectrum of risk.** An adequate consolidated AML/CFT Compliance Program provides the framework for all subsidiaries, business lines and foreign branches to meet their specific regulatory requirements (e.g., country or industry requirements). Accordingly, financial institutions that centrally manage a consolidated AML/CFT Compliance Program should, among other things, provide appropriate structure and advise the business lines, subsidiaries and foreign branches on the development of appropriate guidelines.

An organization applying a consolidated AML/CFT Compliance Program may choose to manage only specific compliance controls (e.g. STR monitoring systems & audit) on a consolidated basis, with other compliance controls managed solely within affiliates, subsidiaries and business lines.

Suspicious Transaction Reporting

Financial institution's holding companies (FIHC) or any non-bank subsidiary thereof, or a foreign owned financial institution that is subject to the BOFI Act or any non-bank subsidiary of such a foreign owned financial institution operating in Nigeria, are required to file STRs. A FIHC's non-bank subsidiaries operating only outside Nigeria are also required to file STRs. Certain savings and loan holding companies and their non depository subsidiaries are required to file STRs pursuant to CBN AML/CFT Regulations 2009. In addition, savings and loan holding companies are strongly required to file STRs.

15. OVERVIEW OF FOREIGN BRANCHES AND OFFICES OF NIGERIAN FINANCIAL INSTITUTIONS

The Financial institution's systems are required to be adequate to manage the risks associated with foreign branches and offices, and the management should have the ability to implement its monitoring and reporting systems effectively.

Nigerian financial institutions open foreign branches and offices in order to meet specific customer demands, help them grow, or expand products or services offered. Foreign branches and offices vary significantly in size, complexity of operations, and scope of products and services offered. Financial institutions must take these factors into consideration when reviewing their foreign branches and offices AML/CFT Compliance Program. Financial institutions are expected to have policies, procedures and processes in place at all their branches and offices to protect against risks of money laundering and terrorist financing. AML/CFT policies, procedures and processes at the foreign office or branch should comply with local requirements and be consistent with the Nigerian financial institution's standards; however, they may need to be tailored for local or business practices.

Risk Factors

Financial institutions should understand the type of products and services offered at their foreign branches and offices, as well as the customers and geographic locations served at the foreign branches and offices. Any service offered by the Nigerian financial institution may be offered by the foreign branches and offices if not prohibited by the host country. Such products and services offered at the foreign branches and offices may have a different risk profile from that of the same products or services offered in Nigerian. Therefore, the institution should be aware that risks associated with foreign branches and offices may differ (e.g., wholesale versus retail operations).

Financial institution should understand the foreign jurisdiction's various AML/CFT requirements. Secrecy laws or their equivalent may affect the ability of the foreign branch or office to share information with the Nigerian financial institutions parent institution. While financial institution with overseas branches or subsidiaries may find it necessary to tailor monitoring approaches as a result of local privacy laws, the compliance oversight mechanism should ensure it can effectively assess and monitor risks within such branches and subsidiaries.

Although specific MLPA requirements are not applicable at foreign branches and offices, financial institutions are expected to have policies, procedures and processes in place at all their branches and offices to protect against risks of money laundering and terrorist financing. In this regard, foreign branches and offices should be guided by the Nigerian financial institutions' AML/CFT policies, procedures and processes. The foreign branches and offices must comply with applicable provisions of Money Laundering Prohibition Act (MLPA), AML/CFT Regulation requirements and all other local AML/CFT related laws, rules and regulations.

Risk Mitigation

Branches and offices of Nigerian financial institutions located in higher-risk geographic locations may be vulnerable to abuse by money launderers. To address this concern, the **Nigerian financial institution's policies, procedures and processes for the foreign operation should be consistent with the following recommendations:**

- i. The Nigerian financial institution's head office and management in Nigeria & the one at the foreign country should understand the effectiveness and quality of supervision and the legal and regulatory requirements of the host country. The Nigerian financial institution's head office should be aware of and understand any concerns that the host country supervisors may have with respect to the foreign branch or office.
- ii. The Nigerian financial institution's head office should understand the foreign branches' or offices' risk profile (e.g., products, services, customers and geographic locations).
- iii. The Nigerian financial institution's head office and management should have access to sufficient information in order to periodically monitor the activity of their foreign branches and offices, including the offices' and branches' level of compliance with head office policies, procedures and processes. Some of this may be achieved through Management Information System (MIS) reports.

The Nigerian financial institution's head office should develop a system for testing and verifying the integrity and effectiveness of internal controls at the foreign branches or offices by conducting in-country audits. Senior management at the head office should obtain and review copies (written in English) of audit reports and any other reports related to AML/CFT and internal control evaluations.

- iv. The Nigeria financial institution's head office should establish robust information-sharing practices between branches and offices, particularly regarding higher-risk account relationships. The institution should use the information to evaluate and understand account relationships throughout the corporate structure (e.g., across borders or legal structures).
- v. The Nigerian institution's head office should be able to provide Examiners with any information deemed necessary to assess compliance with the applicable laws.

Foreign branch and office compliance and audit structures can vary substantially based on the scope of operations (e.g., geographic locations) and the type of products, services and customers. Foreign branches and offices with multiple locations within a geographic region are frequently overseen by branch compliance and audit staff. Regardless of the size or scope of operations, the compliance and audit staff and audit programs should be sufficient to oversee the ML/FT risk.

16. OVERVIEW OF PARALLEL BANKING

The financial institution's systems are required to be adequate to manage the risks associated with parallel banking relationships and the management should have the ability to implement its due diligence, monitoring and reporting systems effectively.

A parallel financial institution exists when at least one Nigerian financial institution and one foreign financial institution are controlled either directly or indirectly by the same person or group of persons who are closely associated in their business dealings or otherwise acting together, but are not subject to consolidated supervision by a single home country supervisor. The foreign financial institution will be subject to different money laundering rules and regulations and a different supervisory oversight structure, both of which may be less stringent than Nigeria. The regulatory and supervisory differences heighten the ML/FT risk associated with parallel banking organizations.

Risk Factors

Parallel banking organizations may have common management, share policies and procedures, cross-sell products, or generally be linked to a foreign parallel financial institution in a number of ways. The key money laundering concern regarding parallel banking organizations is that the Nigerian financial institution may be exposed to greater risk through transactions with the foreign parallel financial institution. Transactions may be facilitated and risks heightened because of the lack of arm's length dealing or reduced controls on transactions between financial institutions that are linked or closely associated. **For example, officers or directors may be common to both entities or may be different but nonetheless work together.**

Risk Mitigation

The Nigerian financial institution's policies, procedures and processes for parallel banking relationships should be consistent with those of other foreign correspondent bank relationships. **In addition, parallel financial institutions should:**

- i. Provide for independent lines of decision-making authority.
- ii. Guard against conflicts of interest.
- iii. Ensure independent and arm's-length dealings between related entities.

17. OVERVIEW OF CORRESPONDENT ACCOUNTS (DOMESTIC)

The financial institution's systems are to be adequate to manage the ML/FT risks associated with offering of domestic correspondent account relationships, and the management must have the ability to implement its monitoring and reporting systems effectively.

Financial institutions maintain correspondent relationships at other domestic financial institutions to provide certain services that can be performed more economically or efficiently because of the other financial institution's size, expertise in a specific line of business or geographic location. **Such services may include:**

- i. **Deposit accounts** - Assets known as "due from financial institution deposits" or "correspondent financial institution balances" may represent the financial institution's primary operating account.
- ii. **Funds transfers** - A transfer of funds between financial institutions may result from the collection of cheques or other cash items, transfer and settlement of securities transactions, transfer of participating loan funds, purchase or sale of government funds, or processing of customer transactions.
- iii. **Other services** - Services include processing of loan participations, facilitating secondary market loan sales, performing data processing and payroll services and exchanging foreign currency.

ML/FT Risk Factors

Because domestic financial institutions must follow the same regulatory requirements, ML/FT risks in domestic correspondent banking are minimal in comparison to other types of financial services, especially for proprietary accounts (i.e., the domestic financial institution is using the correspondent account for its own transactions). Each financial institution, however, has its own approach for conducting its AML/CFT Compliance Program, including customer due diligence, MIS, account monitoring, and reporting suspicious transactions. Furthermore, while a domestic correspondent account may not be considered higher risk, transactions through the account, which may be conducted on behalf of the respondent's customer, may be higher risk. ML/FT risks can be heightened when a respondent financial institution allows its customers to direct or execute transactions through the correspondent account, especially when such transactions are directed or executed through an ostensibly proprietary account.

The correspondent financial institution also faces heightened risks when providing direct currency shipments for customers of respondent financial institution. This is not to imply that such activities necessarily entail money laundering, but these **direct**

currency shipments should be appropriately monitored for unusual and suspicious activity. Without such a monitoring system, the correspondent bank is essentially providing these direct services to an unknown customer.

Risk Mitigation

Financial institutions that offer correspondent bank services to respondent banks should have policies, procedures and processes to manage the ML/FT risks involved in these correspondent relationships and to detect and report suspicious activities. **Financial institution should ascertain whether domestic correspondent accounts are proprietary or allow third-party transactions.** When the respondent financial institution allows third-party customers to transact business through the correspondent account, **the correspondent financial institution should ensure that it puts the necessary steps in understanding the due diligence and procedures of the monitoring applied by the respondent on its customers that will be utilizing the account.**

The level of risk varies depending on the services provided and the types of transactions conducted through the account and the respondent financial institution's AML/CFT Compliance Program, products, services, customers, entities and geographic locations. Each financial institution should appropriately monitor transactions of domestic correspondent accounts relative to the level of assessed risk.

18. OVERVIEW OF CORRESPONDENT ACCOUNTS (FOREIGN)

The Nigerian financial institution's systems are required to be adequate to manage the ML/FT risks associated with foreign correspondent banking and the management should have the ability to implement its due diligence, monitoring and reporting systems effectively.

Foreign financial institutions maintain accounts at Nigerian financial institutions to gain access to the Nigerian financial system and to take advantage of services and products that may not be available in the foreign financial institution's jurisdiction. These services may be performed more economically or efficiently by the Nigerian financial institutions or may be necessary for other reasons, such as the facilitation of international trade.

Services may include:

- i. Cash management services, including deposit accounts.
- ii. International funds transfers.
- iii. Check clearing.
- iv. Payable through accounts.

- v. Pouch activities.
- vi. Foreign exchange services.
- vii. Overnight investment accounts (sweep accounts).
- viii. Loans and letters of credit.

Contractual Agreements

Each relationship that a Nigerian financial institution has with a foreign correspondent financial institution should be governed by an agreement or a contract describing each party's responsibilities and other relationship details (e.g., products and services provided, acceptance of deposits, clearing of items, forms of payment and acceptable forms of endorsement). The agreement or contract should also consider the foreign financial institution's AML/CFT regulatory requirements, customer-base, due diligence procedures and permitted third-party usage of the correspondent account.

ML/FT Risk Factors

Some foreign financial institutions are not subject to the same or similar regulatory guidelines as Nigerian financial institutions; therefore, these foreign institutions may pose a higher money laundering and financing terrorists risk to their respective Nigerian financial institutions correspondent(s). Investigations have disclosed that in the past, foreign correspondent accounts were used to launder funds.

Shell companies are sometimes used in the layering process to hide the true ownership of accounts at foreign correspondent financial institutions. Because of the large amount of funds, multiple transactions, and the Nigerian financial institution's potential lack of familiarity with the foreign correspondent financial institution's customer, criminals and terrorists can more easily conceal the source and use of illicit funds. **Consequently, each Nigerian financial institution, including all overseas branches, offices and subsidiaries should closely monitor transactions related to foreign correspondent accounts.**

Nested Accounts

Nested accounts occur when one foreign financial institution gains access to the financial system in Nigeria by operating through the correspondent account belonging to another foreign financial institution.

If the Nigerian financial institution is unaware that its foreign correspondent financial institution customer is providing such access to third-party foreign financial institutions, these third-party financial institutions can effectively gain anonymous access to the Nigerian financial system. Behaviour indicative of nested accounts and other accounts of concern includes transactions in jurisdictions in which the foreign financial institution has no known business activities or interests and transactions in which the total volume

and frequency significantly exceed expected activity for the foreign financial institution, considering its customer base or asset size.

Risk Mitigation

Nigerian financial institutions that offer foreign correspondent financial institution services should have policies, procedure, and processes to manage the ML/FT risks inherent with these relationships and should closely monitor transactions related to these accounts to detect and report suspicious transactions. The level of risk varies depending on the foreign financial institution's products, services, customers and geographic locations. **The Nigerian financial institutions' policies, procedures and processes should:**

- i. Specify appropriate account-opening procedures and KYC requirements, which may include minimum levels of documentation to be obtained from prospective customers; an account approval process independent of the correspondent account business line for potential higher-risk customers; and a description of circumstances when the financial institution will not open an account.
 - ii. Assess the risks posed by a prospective foreign correspondent customer relationship utilizing consistent, well-documented risk-rating methodologies, and incorporate that risk determination into the financial institution's suspicious transaction monitoring system.
 - iii. Understand the intended use of the accounts and expected account activity (e.g., determine whether the relationship will serve as a payable through account).
 - iv. Understand the foreign correspondent financial institution's other correspondent relationships (e.g., determine whether nested accounts will be utilized).
 - v. Conduct adequate and ongoing due diligence on the foreign correspondent financial institution relationships, which may include periodic visits.
 - vi. Establish a formalized process for escalating suspicious information on potential and existing customers to an appropriate management level for review.
 - vii. Ensure that foreign correspondent financial institution relationships are appropriately included within the Nigerian financial institution's suspicious transaction monitoring and reporting systems.
 - viii. Ensure that appropriate due diligence standards are applied to those accounts determined to be higher risk.
 - ix. Establish criteria for closing the foreign correspondent financial institution account.
- As a sound practice, Nigerian financial institutions are encouraged to communicate their AML/CFT-related expectations to their foreign correspondent financial institutions' customers. Moreover, the Nigerian financial institutions should generally understand the

AML/CFT controls at the foreign correspondent financial institution, including customer due diligence practices and record keeping documentation.

19. OVERVIEW OF BULK SHIPMENTS OF CURRENCY

The Nigerian financial institution's systems are required to be adequate to manage the risks associated with receiving bulk shipments of currency and management should have the ability to implement effective monitoring and reporting systems.

Bulk shipments of currency entail the use of common, independent, or Postal Service's air/land/sea carriers to transport large volumes of bank notes (Nigeria or foreign) from sources either inside or outside Nigeria to a bank in Nigeria. Often, but not always, shipments take the form of containerized cargo.

Shippers may be **"Currency Originators" i.e., individuals or businesses that generate currency from cash sales of commodities or other products or services (including monetary instruments or exchanges of currency).**

Shippers also may be **"intermediaries" that ship currency gathered from their customers who are Currency Originators.** Intermediaries may also ship currency gathered from other intermediaries. Intermediaries may be other financial institutions, central banks, non-deposit financial institutions or agents of these entities.

Financial institutions receive bulk shipments of currency directly when they take possession of an actual shipment. Financial institutions receive bulk shipments of currency indirectly when they take possession of the economic equivalent of a currency shipment, such as through a cash letter notification.

Risk Factors

Bulk shipments of currency to financial institutions from shippers that are presumed to be reputable may nevertheless originate from illicit activity. The monetary proceeds of criminal activities, for example, often reappear in the financial system as seemingly legitimate funds that have been placed and finally integrated by flowing through numerous intermediaries and layered transactions that disguise the origin of the funds. Layering can include shipments to or through other jurisdictions. **Accordingly, financial institutions that receive direct or indirect bulk shipments of currency risk becoming complicit in money laundering or terrorist financing schemes.**

In recent years, the smuggling of bulk currency has become a preferred method for moving illicit funds across borders. However, the activity of shipping currency in bulk is not necessarily indicative of criminal or terrorist activity. Many individuals and businesses, both domestic and foreign, generate currency from

legitimate cash sales of commodities or other products or services. Also, intermediaries gather and ship currency from single or multiple currency originators whose activities are legitimate. Financial institutions may legitimately offer services to receive such shipments. However, financial institutions should be aware of the potential misuse of their services by shippers of bulk currency. Financial institutions also should guard against introducing the monetary proceeds of criminal or terrorist activity into the financial system.

Risk Mitigation

Nigerian financial institutions that offer services to receive bulk shipments of currency should have policies, procedures and processes in place that mitigate and manage the ML/FT risks associated with the receipt of bulk currency shipments. Financial institutions should also closely monitor bulk currency shipment transactions to detect and report suspicious transaction, with particular emphasis on the source of funds and the reasonableness of transaction volumes from currency originators and intermediaries.

ML/FT risk mitigation begins with an effective risk assessment process that distinguishes relationships and transactions that present a higher risk of money laundering or terrorist financing. Risk assessment processes should consider currency originator's and intermediary's ownership, geographies and the nature, source, location and control of bulk currency.

Financial institution's policies, procedures and processes should:

- i. Specify appropriate ML/FT risk-based relationship & account opening procedures which may include minimum levels of documentation to be obtained from prospective currency originators and intermediaries; specify relationship approval process that, for potential higher-risk relationships, is independent of the business line and may include a visit to the prospective shipper or shipping-preparation sites; and describe the circumstances under which the financial institution will not open a relationship.
- ii. Determine the intended use of the relationship, the expected volumes, frequency of activity arising from transactions, sources of funds, reasonableness of volumes based on originators and shippers and any reporting requirements (CTRs, STRs, PEPs, etc).
- iii. Identify the characteristics of acceptable and unacceptable transactions, including circumstances when the bank will or will not accept bulk currency shipments.
- iv. Assess the risks posed by a prospective shipping relationship using consistent and well-documented risk-rating methodologies.

- v. Incorporate risk assessments, as appropriate, into the financial institution's customer due diligence, EDD and suspicious transaction monitoring systems.
- vi. Once the relationship is established, require adequate and ongoing due diligence which, as appropriate, may include periodic visits to the shipper and to shipping-preparation sites. As necessary, scrutinize for legitimacy the root source of cash shipments, using risk-based processes.
- vii. Ensure that appropriate due diligence standards are applied to relationships determined to be higher risk.
- viii. Include procedures for processing shipments, including employees' responsibilities, controls, reconciliation and documentation requirements, and employee/management authorizations.
- ix. Establish a process for escalating suspicious information on potential and existing currency originator and intermediary relationships and transactions to an appropriate management level for review.
- x. Refuse shipments that have questionable or suspicious origins.
- xi. Ensure that shipping relationships and comparisons of expected and actual shipping volumes are included, as appropriate, within the Nigerian financial institution's systems for monitoring and reporting suspicious transaction.
- xii. Establish criteria for terminating a shipment relationship.

As a sound practice, financial institutions should inform currency originators and intermediaries of the AML/CFT-related requirements and expectations that apply to Nigerian financial institutions. The financial institutions also should understand the AML/CFT controls that apply to or are otherwise adopted by the currency originator or intermediary, including any customer due diligence and recordkeeping requirements or practices.

Other financial institutions' controls may also prove useful in protecting financial institution against illicit bulk shipments of currency. These may include effective controls over foreign correspondent banking activity, pouch activity, funds transfers, international automated clearing house transactions and remote deposit capture.

Contractual Agreements

Financial institutions should establish agreements or contracts with currency originators or intermediaries. The agreement or contract should describe each party's responsibilities and other relevant details of the relationship. The agreement or contract should reflect and be consistent with any AML/CFT considerations that apply to the

financial institution, the currency originator or intermediary and the currency originator or intermediary's customers. The agreement or contract should also address expectations about due diligence and permitted third-party usage of the shipper's services. While agreements and contracts should provide for respective AML/CFT controls, obligations and considerations, Nigerian financial institutions cannot shift their AML/CFT responsibilities to others.

20. OVERVIEW OF FOREIGN CURRENCY DENOMINATED DRAFTS

The financial institution's systems are required to be adequate to manage the ML/FT risks associated with foreign currency denominated drafts and the management should have the ability to implement its monitoring and reporting systems effectively.

A foreign currency draft is a financial institution's drafts or cheque denominated in foreign currency and made available at foreign financial institution. These drafts are drawn on a Nigerian correspondent account by a foreign financial institution. Such drafts are frequently purchased to pay for commercial or personal transactions and to settle overseas obligations.

ML/FT Risk Factors

Most foreign currency denominated drafts could be legitimate. However, such drafts have proven to be vulnerable to money laundering abuse. Schemes involving foreign currency drafts could involve the smuggling of currency to a foreign financial institution for the purchase of a cheque or draft denominated in another foreign currency. The foreign financial institution accepts the draft denominated in a particular foreign currency and issues another draft denominated in a different foreign currency. Once the currency is in the form of a bank draft, the money launderer can more easily conceal the source of funds. The ability to convert illicit proceeds to a bank draft at a foreign financial institution makes it easier for a money launderer to transport the instrument either back into the originating country or to endorse it to a third party in a jurisdiction where money laundering laws or compliance are lax. In any case, when the individual has succeeded in laundering his illicit proceeds, the draft or cheque would be returned ultimately for processing in the originating country.

Risk Mitigation

The financial institution's policies, procedures and processes should include the following:

- i. Outline criteria for opening a foreign currency denominated draft relationship with a foreign financial institution or entity (e.g., jurisdiction, products, services, target market, purpose of account and anticipated activity or customer history).
- ii. Detail acceptable and unacceptable transactions (e.g., structuring transactions or the purchase of multiple sequentially numbered drafts for the same payee).
- iii. Detail the monitoring and reporting of suspicious transaction associated with foreign currency denominated drafts.
- iv. Discuss criteria for closing a foreign currency denominated draft relationships.

21. OVERVIEW OF PAYABLE THROUGH ACCOUNTS

The financial institution's systems are required to be adequate to manage the risks associated with payable through accounts (PTA), and the management should have the ability to implement its monitoring and reporting systems effectively.

Foreign financial institutions use PTAs, also known as "pass-through" or "pass-by" accounts to provide their customers with access to the Nigerian financial system. Some financial institutions in Nigeria also offer payable through accounts as a service to foreign financial institutions. The risk associated with money laundering/ financing of terrorism and other illicit activities is higher in PTAs that are not adequately controlled.

Generally, a foreign financial institution requests a PTA for its customers that want to conduct banking transactions in Nigeria through the foreign financial institution's account at financial institution in Nigeria. The foreign financial institution provides its customers, commonly referred to as "**sub account holders,**" with cheques that allow them to draw funds from the foreign financial institution's account from a Nigerian financial institution. The sub account holders, which may number several hundred or in the thousands for one PTA, all become signatories on the foreign financial institution's account in a Nigerian financial institution. While payable through customers are able to write cheques and make deposits at a financial institution in Nigeria like any other account holder, they might not be directly subject to the financial institution's account opening requirements in Nigeria.

PTA activities should not be confused with traditional international correspondent banking relationships in which a foreign financial institution enters into an agreement with a Nigerian financial institution to process and complete transactions on behalf of the foreign financial institution and its customers. Under the latter correspondent arrangement, the foreign financial institution's customers do not have direct access to the correspondent

account at the Nigerian financial institution, but they do transact business through the Nigerian financial institution. This arrangement differs significantly from a PTA with sub accountholders who have direct access to the Nigerian financial system by virtue of their independent ability to conduct transactions with the Nigerian financial system through the PTA.

ML/FT Risk Factors

PTAs may be prone to higher risk because Nigerian financial institutions do not typically implement the same due diligence requirements for PTAs that they require of domestic customers who want to open current and other accounts.

Foreign financial institutions' use of PTAs, coupled with inadequate oversight by Nigerian financial institutions, may facilitate unsound banking practices, including money laundering/ financing of terrorism and other related criminal activities. The potential for facilitating money laundering or terrorist financing, and other serious crimes increases when a Nigerian financial institution is unable to identify and adequately understand the transactions of the ultimate users (all or most of whom are outside of Nigeria) of its account with a foreign correspondent. **PTAs used for illegal purposes can cause financial institutions serious financial losses in criminal and civil fines and penalties, seizure or forfeiture of collateral and reputation damage.**

Risk Mitigation

Financial institutions offering PTA services should develop and maintain adequate policies, procedures and processes to guard against possible illicit use of these accounts. At a minimum, policies, procedures and processes should enable each Nigerian financial institution to identify the ultimate users of its foreign financial institution's PTA. **This should include the financial institution's obtaining (or having the ability to obtain through a trusted third-party arrangement) substantially the same information on the ultimate PTA users as it obtains on its direct customers.**

Policies, procedures and processes should include a review of the foreign financial institution's processes to identify and monitor the transactions of its sub-account holders and to comply with any AML/CFT statutory and regulatory requirements existing in Nigeria (as the host country). **It should also review the foreign financial institution's master agreement with the Nigerian financial institutions on the PTAs.** In addition, Nigerian financial institutions should have procedures for monitoring transactions conducted in the foreign financial institutions' PTAs.

In an effort to address the risk inherent in PTAs, financial institutions in Nigeria should have a signed contract (i.e., master agreement) that includes:

- i. Roles and responsibilities of each party.
- ii. Limits or restrictions on transaction types and amounts (e.g., currency deposits, funds transfers, cheque cashing).
- iii. Restrictions on some types of sub accountholders (e.g., finance companies, funds remitters or other non-bank financial institutions).
- iv. Prohibitions or restrictions on multi-tier sub accountholders.
- v. Access to the foreign financial institution's internal documents and audits that pertain to its PTA activity.

Financial institutions should consider closing the PTA in the following circumstances:

- i. Insufficient information on the ultimate PTA users.
- ii. Evidence of substantive or ongoing suspicious activity.
- iii. Inability to ensure that the PTAs are not being used for money laundering or other illicit purposes.

22. OVERVIEW OF POUCH ACTIVITIES

The financial institution's systems are required to be adequate to manage the ML/FT risks associated with pouch activities and the management should have the ability to implement its monitoring and reporting systems effectively.

Pouch activity entails the use of a carrier, courier (either independent or common) or a referral agent employed by the courier to transport currency, monetary instruments and other documents from foreign countries to financial institutions in Nigeria.

Pouches can be sent by financial institution or individuals. Pouch services are commonly offered in conjunction with foreign correspondent banking services. Pouches can contain loan repayments, transactions for demand deposit accounts or other types of transactions.

Risk Factors

Financial institutions should be aware that bulk amounts of monetary instruments purchased in Nigeria that appear to have been structured to avoid the AML/CFT-reporting requirements often have been found in pouches or cash letters received from foreign financial institutions. **The monetary instruments involved are frequently traveller's cheques and bank cheques that usually have one or more of the following characteristics in common:**

- i. The instruments purchased on the same or consecutive days at different locations.
- ii. The payee lines are left blank or made out to the same person (or to only a few people).
- iii. They contain little or no purchaser information.
- iv. They bear the same stamp, symbol or initials.
- v. They are purchased in round denominations or repetitive amounts.
- vi. The depositing of the instruments is followed soon after by a funds transfer out in the same dollar amount.

Risk Mitigation

Financial institutions should have policies, procedures and processes related to pouch activity that should:

- i. Outline criteria for opening a pouch relationship with an individual or a foreign financial institution (e.g., customer due diligence requirements, type of institution or person, acceptable purpose of the relationship).
- ii. Detail acceptable and unacceptable transactions (e.g., monetary instruments with blank payees, unsigned monetary instruments and a large number of consecutively numbered monetary instruments).
- iii. Detail procedures for processing the pouch including employee responsibilities, dual control, reconciliation, documentation requirements, and employee sign off.
- iv. Detail procedures for reviewing of unusual or suspicious transaction including elevating concerns to management. Contents of pouches may be subject to CTR, Report of International Transportation of Currency or Monetary Instruments (CMIR).
- v. Discuss criteria for closing pouch relationships.

The above factors should be included within an agreement or contract between the financial institution and the courier that details the services to be provided and the responsibilities of both parties.

23. OVERVIEW OF ELECTRONIC BANKING

The financial institution's systems should be adequate to manage the risks associated with electronic banking (e-banking) customers including **Remote Deposit Capture (RDC) activity** and the management should have the ability to implement its monitoring and reporting systems effectively.

E-banking systems which provide electronic delivery of banking products to customers include automated teller machine (ATM) transactions; online account opening; internet banking transactions; and telephone banking. For example, credit cards, deposit accounts, mortgage loans and funds transfers can all be initiated online without face-to-face contact. **Management needs to recognize this as a potentially higher-risk area and develop adequate policies, procedures and processes for customer identification and monitoring for specific areas of banking.**

ML/FT Risk Factors

Financial institutions should ensure that their monitoring systems adequately capture transactions conducted electronically. As with any account, they should be alert to anomalies in account behaviour. **Red flags may include the velocity of funds in the account or in the case of ATMs, the number of debit cards associated with the account.**

Accounts that are opened without face-to-face contact may be a higher risk for money laundering and terrorist financing for the following reasons:

- i. More difficult to positively verify the individual's identity.
- ii. Customer may be out of the financial institution's targeted geographic area or country.
- iii. Customer may perceive the transactions as less transparent.
- iv. Transactions are instantaneous.
- v. May be used by a "front" company or unknown third party.

Risk Mitigation

Financial institutions should establish AML/CFT monitoring, identification and reporting for unusual and suspicious transactions occurring through e-banking systems. **Useful MIS for detecting unusual transaction in higher-risk accounts include ATM activity reports, funds transfer reports, new account activity reports, change of internet address reports, Internet Protocol (IP) address reports and reports to identify related or linked accounts (e.g., common addresses, phone numbers, e-mail addresses and tax identification numbers).**

In determining the level of monitoring required for an account, financial institutions should include how the account was opened as a factor. Financial institutions engaging in transactional internet banking **should have effective and reliable methods to authenticate a customer's identity when opening accounts online and should establish policies for when a customer should be required to open accounts on a face-to-face basis.** Financial institutions may also institute other controls, such as establishing transaction dollar limits for large items that require manual intervention to exceed the pre-set limit.

Remote Deposit Capture

Remote Deposit Capture (RDC) is a deposit transaction delivery system that has made cheque and monetary instrument processing (e.g., traveller's cheques) more efficient.

In broad terms, RDC allows a financial institution's customers to scan a cheque or monetary instrument and then transmit the scanned or digitized image to the institution.

It should be noted that scanning and transmission activities can take place at remote locations including the financial institution's branches, ATMs, domestic and foreign correspondents, and locations owned or controlled by commercial or retail customers. By eliminating face-to-face transactions, RDC decreases the cost and volume of paper associated with physically mailing or depositing items. RDC also supports new and existing banking products and improves customers' access to their deposits.

ML/FT Risk Factors in Remote Deposit Capture

RDC may expose financial institutions to various risks including money laundering, financing of terrorists, fraud and information security. Fraudulent, sequentially numbered or physically altered documents, particularly money orders and traveler's cheques may be more difficult to detect when submitted by RDC and not inspected by a qualified person. Financial institutions may face challenges in controlling or knowing the location of RDC equipment because the equipment can be readily transported from one jurisdiction to another.

This challenge is increased as foreign correspondents and foreign money services businesses are increasingly using RDC services to replace pouch and certain instrument processing and clearing activities. Inadequate controls could result in intentional or unintentional alterations to deposit item data, re-submission of a data file, or duplicate

presentation of cheques and images at one or multiple financial institutions. In addition, original deposit items are not typically forwarded to financial institutions, but instead the customer or the customer's service provider retains them. As a result, recordkeeping, data safety and integrity issues may increase.

Higher-risk customers may be defined by industry, incidence of fraud or other criteria. Examples of higher-risk parties include online payment processors, certain credit-repair services, certain mail order and telephone order companies, online gambling operations, businesses located offshore and adult entertainment businesses.

Risk Mitigation

Management should develop appropriate policies, procedures and processes to mitigate the risks associated with RDC services and to effectively monitor for unusual or suspicious transactions. Examples of risk mitigants include:

- i. Comprehensively identifying and assessing RDC risk prior to implementation. Senior management should identify AML/CFT operational, information security, compliance, legal, and reputation risks. Depending on the financial institution's size and complexity, this comprehensive risk assessment process should include staff from information technology and security, deposit operations, treasury or cash management sales, business continuity, audit, compliance, accounting and legal.
- ii. Conducting appropriate CDD and EDD.
- iii. Creating risk-based parameters that can be used to conduct Remote Deposit Capture (RDC) customer suitability reviews. Parameters may include a list of acceptable industries, standardized underwriting criteria (e.g., credit history, financial statements and ownership structure of business) and other risk factors. When the level of risk warrants, financial institutions' staff should consider visiting the customer's physical location as part of the suitability review. During these visits, the customer's operational controls and risk management processes should be evaluated.
- iv. Conducting vendor due diligence when financial institutions use a service provider for RDC activities. Management should ensure implementation of sound vendor management processes.
- v. Obtaining expected account activity from the RDC customer, such as the anticipated RDC transaction volume, and type (e.g., payroll cheques, third-party cheques, or traveller's cheques), comparing it to actual transaction and resolving significant deviations. Comparing expected activity to business type to ensure they are reasonable and consistent.
- vi. Establishing or modifying customer Remote Deposit Capture transaction limits.
- vii. Developing well-constructed contracts that clearly identify each party's role, responsibilities and liabilities, and detail record retention procedures for RDC

data. These procedures should include physical and logical security expectations for access, transmission, storage and ultimate disposal of original documents. The contract should also address the customer's responsibility for properly securing RDC equipment and preventing inappropriate use, including establishing effective equipment security controls (e.g., passwords & dual control access). In addition, contracts should detail the RDC customer's obligation to provide original documents to the financial institution in order to facilitate investigations related to unusual transactions or poor quality transmissions, or to resolve disputes. Contracts should clearly detail the authority of the financial institution to mandate specific internal controls, conduct audits or terminate the RDC relationship. Implementing additional monitoring or review when significant changes occur in the type or volume of transactions, or when significant changes occur in the underwriting criteria, customer base, customer risk management processes or geographic location that the bank relied on when establishing RDC services.

- viii. Ensuring that RDC customers receive adequate training. The training should include documentation that addresses issues such as routine operations and procedures, duplication and problem resolution.
- ix. Using improved aggregation and monitoring capabilities as facilitated by the digitized data.
- x. As appropriate, using technology to minimize errors (e.g., the use of franking to stamp or identify a deposit as being processed).

24. OVERVIEW OF FUNDS TRANSFERS

The financial institution's systems should be adequate to manage the ML/FT risks associated with funds transfers and the management should have ability to implement effective monitoring and reporting systems effectively.

Payment systems in Nigeria consist of numerous financial intermediaries, financial services companies and non-bank businesses that create process and distribute payments. The domestic and international expansion of the financial industry services has increased the importance of electronic funds transfers, including funds transfers made through the wholesale payment systems.

Funds Transfer Services

The vast majority of the value of Naira payments or transfers in Nigeria is ultimately processed through wholesale payment systems which generally handle large-value transactions between financial institutions. Financial institutions conduct these transfers on their own behalf as well as for the benefit of other financial service providers and financial institution customers, both consumer and corporate.

Related retail transfer systems facilitate transactions such as automated clearing houses (ACH); automated teller machines (ATM); point-of-sales (POS); telephone bill paying; home banking systems; and credit, debit, and prepaid cards. Most of these retail transactions are initiated by customers rather than by financial institutions or corporate users. These individual transactions may then be batched in order to form larger wholesale transfers, which are the focus of this section.

The primary domestic wholesale payment system for interbank funds transfers is the **Nigerian Inter-Bank Settlement System (NIBSS)**. The bulk of the Naira value of these payments is originated electronically to make large value, time-critical payments, such as the settlement of interbank purchases and sales of government funds, settlement of foreign exchange transactions, disbursement or repayment of loans; settlement of real estate transactions or other financial market transactions; and purchasing, selling or financing securities transactions. NIBSS and **Real Time Gross Settlement System (RTGS)** participants facilitate these transactions on their behalf and on behalf of their customers, including non-bank financial institutions, commercial businesses and correspondent banks that do not have direct access.

Structurally, there are two components to funds transfers:

- i. The instructions, which contain information on the sender and receiver of the funds; and
- ii. The actual movement or transfer of funds.

The instructions may be sent in a variety of ways, including by electronic access to networks operated by the NIBSS payment systems; by access to financial telecommunications systems such as **Society for Worldwide Interbank Financial Telecommunication (SWIFT)**; or e-mail, facsimile, telephone or telex.

NIBSS and RTGS are used to facilitate funds transfers between two domestic endpoints or the fund segment of international transactions. SWIFT is an international messaging service that is used to transmit payment instructions for the vast majority of international interbank transactions which can be denominated in numerous currencies.

Society for Worldwide Interbank Financial Telecommunication

The SWIFT network is a messaging infrastructure (not a payments system) which provides users with a private international communications-link among themselves.

The actual funds movements (payments) are completed through correspondent financial institution relationship. Movement of payments denominated in different currencies occurs through correspondent financial institution relationships or over funds transfer systems in the relevant country. In addition to customer and financial

institution funds transfers, SWIFT is used to transmit foreign exchange confirmations, debit and credit entry confirmations, statements, collections and documentary credits.

Cover Payments

A typical funds transfer involves an originator instructing his financial institution (the originator's financial institution) to make payment to the account of a payee (the beneficiary) in the beneficiary's financial institution. **A cover payment occurs when the originator's financial institution and the beneficiary's financial institution do not have a relationship that allows them to settle the payment directly. In that case, the originator's financial institution instructs the beneficiary's financial institution to effect the payment and advises that transmission of funds to "cover" the obligation created by the payment order has been arranged through correspondent accounts at one or more intermediary financial institutions.**

Cross-border cover payments usually involve multiple financial institutions in multiple jurisdictions.

Informal Value Transfer System

An Informal Value Transfer System (**IVTS**) is used to describe a currency or value transfer system that operates informally to transfer money as a business. In countries lacking a stable financial sector or with large areas not served by formal financial institutions, IVTS may be the only method for conducting financial transactions. Persons living in Nigeria may use IVTS to transfer funds to their home countries.

Payable Upon Proper Identification Transactions

One type of funds transfer transaction that carries particular ML/FT risk is the payable upon proper identification (PUPID) service. **PUPID transactions are funds transfers for which there are no specific account to deposit the funds into and the beneficiary of the funds is not a financial institution customer.**

For example, an individual may transfer funds to a relative or an individual who does not have an account relationship with the financial institution that receives the funds transfer. In this case, the beneficiary financial institution may place the incoming funds into a suspense account and ultimately release the funds when the individual provides proof of identity. In some cases, financial institutions permit non-customers to initiate PUPID transactions. **These transactions are considered extremely high risk and require strong controls.**

ML/FT Risk Factors in Funds Transfer

Funds transfers may present a heightened degree of ML/FT risk, depending on such factors as the number and Naira volume of transactions, geographic location of originators and beneficiaries, and whether the originator or beneficiary is a financial institution customer. The size and complexity of a financial institution's operation and the origin and destination of the funds being transferred will determine which type of funds transfer system the financial institution uses. The vast majority of funds transfer instructions are conducted electronically. However, Examiners need to be mindful that physical instructions may be transmitted by other informal methods, as described earlier.

Cover payments made through SWIFT pose additional risks for intermediary financial institutions that do not have facilities that identify the originator and beneficiary of the funds transfer. Without such facilities, the intermediary financial institution is unable to monitor or filter payment information. This lack of transparency limits the Nigerian intermediary financial institution's ability to appropriately assess and manage the risk associated with correspondent and clearing operations and monitor suspicious transaction.

The risks of PUPID transactions to the beneficiary financial institution are similar to other transactions in which the financial institution does business with non-customers. However, the risks are heightened in PUPID transactions if the financial institution allows a non-customer to access the funds transfer system by providing minimal or no identifying information. **Financial institutions that allow non-customers to transfer funds using the PUPID service pose significant risk to both the originating and beneficiary financial institution. In these situations, both financial institutions have minimal or no identifying information on the originator or the beneficiary.**

Risk Mitigation

Funds transfers can be used in the placement, layering and integration stages of money laundering. Funds transfers purchased with currency are an example of the placement stage. Detecting unusual transaction in the layering and integration stages is more difficult for a financial institution because transactions may appear legitimate. In many cases, a financial institution may not be involved in the placement of the funds or in the final integration, only the layering of transactions. Financial institutions should consider all three stages of money laundering when evaluating or assessing funds transfer risks.

Financial institutions need to have sound policies, procedures and processes to manage the ML/FT risks of its funds transfer activities. Funds transfer policies, procedures and processes should address all foreign correspondent banking

transactions, including transactions in which Nigerian branches and agencies of foreign financial institutions are intermediaries for their head offices.

Obtaining CDD information is an important risk mitigant in providing funds transfer services. Because of the nature of funds transfers, adequate and effective CDD policies, procedures and processes are critical in detecting unusual and suspicious transactions. An effective risk-based suspicious transaction monitoring and reporting system is equally important. Whether this monitoring and reporting system is automated or manual, it should be sufficient to detect suspicious trends and patterns typically associated with money laundering.

Financial institutions involved in international payments transactions are encouraged to adhere to the following:

- i. Financial institutions should not omit, delete or alter information in payment messages or orders for the purpose of avoiding detection of that information by any other financial institution in the payment process;
- ii. Financial institutions should not use any particular payment message for the purpose of avoiding detection of information by any other financial institution in the payment process;
- iii. Subject to all applicable laws, financial institutions should cooperate as fully as practicable with other financial institutions in the payment process when requested to provide information about the parties involved; and
- iv. Financial institutions should strongly encourage their correspondent financial institutions to observe these principles.

In addition, effective monitoring processes for cover payments include:

- i. Monitoring funds transfers processed through automated systems in order to identify suspicious transaction. This monitoring may be conducted after the transfers are processed, on an automated basis, and may use a risk-based approach; and
- ii. Given the volume of messages and data for large Nigerian intermediary financial institutions, a manual review of every payment order may not be feasible or effective. However, intermediary financial institutions should have, as part of their monitoring processes, a risk-based method to identify incomplete fields or fields with meaningless data. **Nigerian financial institutions engaged in processing cover payments should have policies to address such circumstances, including those that involve systems other than SWIFT.**

Originating and beneficiary financial institutions should establish effective and appropriate policies, procedures and processes for PUPID transaction including:

- i. Specifying the type of identification that is acceptable.
- ii. Maintaining documentation of individuals consistent with the bank's recordkeeping policies.
- iii. Defining which financial institution employees may conduct PUPID transactions
- iv. Establishing limits on the amount of funds that may be transferred to or from the financial institution for non-customers.
- v. Monitoring and reporting suspicious transactions.
- vi. Providing enhanced scrutiny for transfers to or from certain jurisdictions.
- vii. Identifying disbursement method for proceeds from a beneficiary financial institution.

25.OVERVIEW OF AUTOMATED CLEARING HOUSE (ACH) TRANSACTIONS

The financial institution's systems should be adequate to manage the risks associated with automated clearing house (ACH) and international ACH transactions (IAT) and the management should have the ability to implement its monitoring and reporting systems effectively.

The use of the ACH has grown markedly over the last several years due to the increased volume of electronic cheque conversion and one-time ACH debits, reflecting the lower cost of ACH processing relative to cheque processing. Cheque conversion transactions as well as one-time ACH debits are primarily of low currency value used for consumer transactions for purchases of goods and services or payment of consumer bills. **ACH is primarily used for domestic payments.**

ACH Payment Systems

Traditionally, the ACH system has been used for the direct deposit of payroll and government benefit payments and for the direct payment of mortgages and loans. As noted earlier, the ACH has been expanding to include one-time debits and cheque conversion. ACH transactions are payment instructions to either credit or debit a deposit account. Examples of credit payment transactions include payroll direct deposit, social security, dividends and interest payments. Examples of debit transactions include mortgage, loan, insurance premium and a variety of other consumer payments initiated through merchants or businesses.

In the electronic cheque conversion process, merchants that receive a cheque for payment do not collect the cheque through the cheque collection system, either electronically or in paper form. Instead, merchants use the information on the cheque to initiate a type of electronic funds transfer known as an ACH debit to the cheque writer's account. The cheque is used to obtain the bank routing number, account number, cheque serial number and currency amount for the transaction. The cheque itself is not sent through the cheque collection system in any form as a payment instrument. Merchants use electronic cheque conversion because it can be a more efficient way for them to obtain payment than collecting the cheque.

RTGS is a central clearing facility for transmitting and receiving ACH payments and SWIFT/ Interswitch which sends cross-border ACH credits and debit payments to some countries around the world.

Third-Party Service Providers

A Third-Party Service Provider (**TPSP**) is an entity other than an originator, Originating Depository Financial Institution (ODFI) or **Receiving Depository Financial Institution (RDFI)** that performs any functions on behalf of the Originator, the ODFI or the RDFI with respect to the processing of ACH entries.

Risk Factors

The ACH system was designed to transfer a high volume of domestic currency transactions which pose lower ML/FT risks. Nevertheless, the ability to send high international currency transactions through the ACH may expose banks to higher ML/FT risks. Banks/Other financial institutions (OFIs) without a robust ML/FT monitoring system may be exposed to additional risk particularly when accounts are opened over the internet without face-to face contact.

ACH transactions that are originated through a TPSP (that is, when the originator is not a direct customer of the ODFI) may increase ML/FT risks, therefore, making it difficult for an ODFI to underwrite and review originator's transactions for compliance with AML/CFT rules. Risks are heightened when neither the TPSP nor the ODFI performs due diligence on the companies for whom they are originating payments.

Certain ACH transactions, such as those originated through the internet or the telephone may be susceptible to manipulation and fraudulent use. Certain practices associated with how the banking industry processes ACH transactions may expose banks/OFIs to ML/FT risks. **These practices include:**

- i. An Originating Depository Financial Institution (ODFI) authorizing a Third Party Service Provider (TPSP) to send ACH files directly to an ACH Operator, in essence by-passing the ODFI.
- ii. ODFIs and Receiving Depository Financial Institutions (RDFIs) relying on each other to perform adequate due diligence on their customers.
- iii. Batch processing that obscures the identities of originators.
- iv. Lack of sharing of information on or about originators and receivers inhibits a bank's/OFIs' ability to appropriately assess, monitor, control/manage and mitigate the risk associated with correspondent and ACH processing operations, monitor for suspicious activity and screen for MLPA 2004 and CBN AML/CFT Regulation 2009 compliance.

Risk Mitigation

The BOFIA 1991 (as amended), MLPA 2004 and CBN AML/CFT Regulation 2009 require financial institutions to have AML/CFT Compliance Programs and appropriate policies, procedures and processes in place to monitor and identify unusual activity, including ACH transactions. Obtaining CDD information in all operations is an important mitigant to ML/FT risk in ACH transactions. Because of the nature of ACH transactions and the reliance that ODFIs and RDFIs place on each other for regulatory reviews and other necessary due diligence information, it is essential that all parties have a strong CDD program for regular ACH customers. For relationships with TPSPs, CDD on the TPSP can be supplemented with due diligence on the principals associated with the TPSP and, as necessary, on the originators.

Adequate and effective CDD policies, procedures and processes are critical in detecting a pattern of unusual and suspicious activities because the individual ACH transactions are typically not reviewed. Equally important is an effective risk-based suspicious activity monitoring and reporting system. In cases where a financial institution is heavily reliant upon the TPSP, the financial institution may want to review the TPSP's suspicious activity monitoring and reporting program, either through its own or an independent inspection. The ODFI may establish an agreement with the TPSP, which delineates general TPSP guidelines, such as compliance with ACH operating requirements and responsibilities and meeting other applicable regulations. **Financial institutions may need to consider controls to restrict or refuse ACH services to potential originators and receivers engaged in questionable or deceptive business practices.**

ACH transactions can be used in the layering and integration stages of money laundering. Detecting unusual activity in the layering and integration stages can be a difficult task, because ACH may be used to legitimize frequent and recurring transactions. **Financial institutions should consider the layering and integration stages of money laundering when evaluating or assessing the ACH transaction risks of a particular customer.**

The ODFI should be aware of IAT activity and evaluate the activity using a risk-based approach in order to ensure that suspicious activity is identified and monitored. The ODFI, if frequently involved in international transfers, may develop a separate process which may be automated for reviewing international transfers that minimizes disruption to general ACH processing, reconciliation and settlement.

The potentially higher risk inherent in international transfers should be considered in the financial institution's ACH policies, procedures and processes. The financial institution should consider its current, potential roles and responsibilities when developing internal controls to monitor and mitigate the risk associated with international transfers and to comply with the financial institution's suspicious activity reporting obligations.

In processing international transfers, financial institutions should consider the following:

- i. Customers and transaction types and volume.
- ii. Third-party payment processor relationships.
- iii. Responsibilities, obligations and risks of becoming a **Gateway Operator (GO)**.
- iv. CIP, CDD and EDD standards and practices.
- v. Suspicious activity monitoring and reporting.
- vi. Appropriate MIS, including the potential necessity for systems upgrades or changes.
- vii. Processing procedures (e.g., identifying and handling international transfers and handling non-compliant and rejected messages).
- viii. Training programs for appropriate bank personnel (e.g., ACH personnel, operations, compliance audit, customer service, etc.).
- ix. Legal agreements, including those with customers, third-party processors and vendors, and whether those agreements need to be upgraded or modified.

Financial institutions that have relationships with third-party service providers should assess the nature of those relationships and their related ACH transactions to ascertain the financial institution's level of ML/FT risk and to develop appropriate policies, procedures and processes to mitigate that risk.

26. OVERVIEW OF ELECTRONIC CASH

The financial institution's systems should be adequate to manage the risks associated with electronic cash (e-cash) and the management should have the ability to implement its monitoring and reporting systems effectively.

E-cash (e-money) is a digital representation of money. E-cash comes in several forms including computer-based, mobile telephone-based and

prepaid cards. Computer e-cash is accessed through personal computer hard disks via a modem or stored-in-an-online repository. Mobile telephone-based e-cash is accessed through an individual's mobile telephone. Prepaid cards, discussed in more detail below, are used to access funds generally held by issuing financial institutions in pooled accounts.

In the case of computer e-cash, monetary value is electronically deducted from the financial institution account when a purchase is made or funds are transferred to another person.

Risk Factors

Transactions using e-cash may pose the following unique risks to the financial institution:

- i. Funds may be transferred to or from an unknown third party.
- ii. Customers may be able to avoid border restrictions as the transactions can become mobile and may not be subject to jurisdictional restrictions.
- iii. Transactions may be instantaneous.
- iv. Specific cardholder activity may be difficult to determine by reviewing activity through a pooled account.
- v. The customer may perceive the transactions as less transparent.

Risk Mitigation

Financial institutions should establish AMLCFT monitoring, identification and reporting for unusual and suspicious activities occurring through e-cash. Useful MIS for detecting unusual activity on higher-risk accounts include **ATM activity reports (focusing on foreign transactions), funds transfer reports, new account activity reports, change of internet address reports, internet protocol (IP) address reports & reports to identify related or linked accounts (e.g., common addresses, phone numbers, e-mail addresses and taxpayer identification numbers)**. The financial institution also may institute other controls, such as establishing transaction and account/currency limits that require manual intervention to exceed the preset limit.

Prepaid Cards/Stored Value Cards

Consistent with industry practice, the term "**prepaid card**" is primarily used in this document. Although some sources use the term "**stored value card**" more broadly, **it most commonly refers to cards where the monetary value is physically stored on the card.**

The term "prepaid card" generally refers to an access device linked to funds held in a pooled account, which is the type of product most frequently offered by banking organizations. Prepaid cards can cover a variety of products,

functionalities and technologies. Prepaid cards operate within either an “open” or “closed” system.

Open-system prepaid cards can be used for purchases at any merchant or to access cash at any automated teller machine (ATM) that connects to the affiliated global payment network. Examples of open system cards are payroll cards and gift cards that can be used anywhere a credit card can be used. Some prepaid cards may be reloaded, allowing the cardholder to add value.

Closed-system cards generally can only be used to buy goods or services from the merchant issuing the card or a select group of merchants or service providers that participate in a specific network. Examples of closed system cards include merchant-specific retail gift cards, mall cards and mass transit system cards.

Some prepaid card programs may combine multiple features, such as a flexible spending account card that can be used to purchase specific health services as well as products at a variety of merchants. These programs are often referred to as “hybrid” cards.

Prepaid cards provide a compact and transportable way to maintain and access funds. They also offer individuals without bank accounts an alternative to cash and money orders. As an alternate method of cross-border funds transmittal, prepaid card programs may issue multiple cards per account, so that persons in another country or jurisdiction can access the funds loaded by the original cardholder via ATM withdrawals of cash or merchant purchases.

Many financial institution that offer prepaid card programs do so as issuer or issuing bank. Most payment networks require that their branded prepaid cards be issued by a bank that is a member of that payment network. In addition to issuing prepaid cards, banks may participate in other aspects of a card program such as marketing and distributing cards issued by another financial institution. Banks often rely on multiple third parties to accomplish the design, implementation and maintenance of their prepaid card programs. These third parties may include program managers, distributors, marketers, merchants and processors. Under payment network requirements, the issuing bank or other financial institution may have due diligence and other responsibilities relative to these third parties.

Contractual Agreements

Each relationship that a Nigerian financial institution has with another financial institution or third party as part of a prepaid card program should be governed by an agreement or a contract describing each party’s responsibilities and other relationship details, such as the products and services provided. The agreement or contract should also consider each party’s AML/CFT compliance requirements, customer base, due diligence procedures and any

payment network obligations. The issuing bank or financial institution maintains ultimate responsibility for AML/CFT compliance whether or not a contractual agreement has been established.

Risk Factors

Money laundering, terrorist financing and other criminal activities may occur through prepaid card programs if effective controls are not in place. **Investigations have found that some prepaid cardholders used false identification and funded their initial deposits with stolen credit cards or purchased multiple cards under aliases.** In the placement phase of money laundering, because many domestic and offshore financial institutions offer cards with currency access through ATMs internationally, criminals may load cash from illicit sources onto prepaid cards through unregulated load points and send the cards to their accomplices inside or outside the country. Investigations have disclosed that both open and closed system prepaid cards have been used in conjunction with, or as a replacement to bulk cash smuggling. Third parties involved in prepaid card programs may or may not be subject to regulatory requirements, oversight and supervision. In addition, these requirements may vary by party.

Prepaid card programs are extremely diverse in the range of products and services offered and the customer bases they serve. In evaluating the risk profile of a prepaid card program, financial institutions should consider the program's specific features and functionalities. No single indicator is necessarily determinative of lower or higher ML/FT risk. Higher potential money laundering risk associated with prepaid cards results from the anonymity of the cardholder, fictitious cardholder information, cash access of the card (especially internationally) and the volume of funds that can be transacted on the card. Other risk factors include type and frequency of card loads and transactions, geographic location of card activity, relationships with parties in the card program, card value limits, distribution channels and the nature of funding sources.

Risk Mitigation

Financial institutions that offer prepaid cards or otherwise participate in prepaid card programs should have policies, procedures and processes sufficient to control and manage the related ML/FT risks. Customer due diligence is an important mitigant of ML/FT risk in prepaid card programs. **A financial institution's CDD program should provide for a risk assessment of all third parties involved in the prepaid card program, considering all relevant factors, including, as appropriate:**

- i. The identity and location of all third parties involved in the prepaid card program, including any sub-agents.
- ii. Corporate documentation, licences, references (including independent reporting services) and, if appropriate, documentation on principal owners.

- iii. The nature of the third-parties' businesses and the markets and customer bases served.
- iv. The information collected to identify and verify cardholder identity.
- v. The type, purpose and anticipated activity of the prepaid card program.
- vi. The nature and duration of the financial institution's relationship with third parties in the card program.
- vii. The ML/FT risk obligations of third parties.

As part of their system of internal controls, financial institutions should establish a means for monitoring, identifying and reporting suspicious activity related to prepaid card programs. This reporting obligation extends to all transactions by, at or through the financial institution, including those in an aggregated form. Financial institutions may need to establish protocols to regularly obtain card transaction information from processors or other third parties. Monitoring systems should have the ability to identify foreign card activity, bulk purchases made by one individual and multiple purchases made by related parties. In addition, procedures should include monitoring for unusual activity patterns, such as cash card loads followed immediately by withdrawals of the full amount from another location.

Card features can provide important mitigation to the ML/FT risks inherent in prepaid card relationships and transactions and may include:

- i. Limits or prohibitions on cash loads, access or redemption.
- ii. Limits or prohibitions on amounts of loads and number of loads/reloads within a specific time frame (velocity or speed of fund use).
- iii. Controls on the number of cards purchased by one individual.
- iv. Maximum currency thresholds on ATM withdrawals and on the number of withdrawals within a specific time frame (velocity or speed of fund use).
- v. Limits or prohibitions on certain usage (e.g., merchant type) and on geographic usage, such as outside Nigeria.
- vi. Limits on aggregate card values.

27. OVERVIEW OF THIRD-PARTY PAYMENT PROCESSORS

The financial institution's systems should be adequate to manage the risks associated with its relationships with third-party payment processors and the management should have the ability to implement its monitoring and reporting systems effectively.

Non-bank or third-party payment processors (processors) are bank or other financial institution customers that provide payment-processing services to merchants and other business entities. Traditionally, processors primarily contract with retailers that have physical locations in order to process the retailers' transactions.

These merchant transactions primarily included credit card payments but also covered automated clearing house (ACH) transactions, **Remotely Created Cheques (RCCs)**, debit and prepaid cards transactions. With the expansion of the internet, retail borders have been eliminated. Processors now provide services to a variety of merchant accounts, including conventional retail and internet-based establishments, prepaid travel, telemarketers and internet gaming enterprises.

Third-party payment processors often use their commercial bank accounts to conduct payment processing for their merchant clients. For example, the processor may deposit into its account RCCs generated on behalf of a merchant client, or act as a third-party sender of ACH transactions. In either case, the financial institution does not have a direct relationship with the merchant. The increased use by processor customers, particularly telemarketers of RCCs also raises the risk of fraudulent payments being processed through the processor's bank account.

Risk Factors

Processors generally are not subject to AML/CFT compliance and regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, fraud schemes and illicit transactions or transactions prohibited by MLPA 2004.

The financial institution's ML/FT risks when dealing with a processor account are similar to risks from other activities in which the financial institution's customer conducts transactions through the bank on behalf of the customer's clients. When the financial institution is unable to identify and understand the nature and source of the transactions processed through an account, the risks to the financial institution and the likelihood of suspicious activity can increase. If a financial institution has not implemented an adequate processor-approval program that goes beyond credit risk management, it could be vulnerable to processing illicit or sanction-able transactions.

Risk Mitigation

Financial institutions offering account services to processors should develop and maintain adequate policies, procedures and processes to address risks related to these relationships. At a minimum, these policies should authenticate the processor's business operations and assess their risk level. **A financial institution may assess the risks associated with payment processors by considering the following:**

- i. Implementing a policy that requires an initial background check of the processor (using for example, state incorporation departments, internet searches and other investigative processes) and of the processor's underlying merchants on a risk-adjusted basis in order to verify their creditworthiness and general business practices.

- ii. Reviewing the processor's promotional materials, including its Web site to determine the target clientele. A financial institution may develop policies, procedures and processes that restrict the types of entities for which it will allow processing services. These entities may include higher risk entities such as offshore companies, online gambling-related operations, telemarketers and online pay lenders. These restrictions should be clearly communicated to the processor at account opening stage.
- iii. Determining whether the processor re-sells its services to a third party who may be referred to as an agent or provider of independent sales institution opportunities or internet service provider (gateway) arrangements.
- iv. Reviewing the processor's policies, procedures and processes to determine the adequacy of its due diligence standards for new merchants.
- v. Requiring the processor to identify its major customers by providing information such as the merchant's name, principal business activity and geographic location.
- vi. Verifying directly or through the processor that the merchant is operating a legitimate business by comparing the merchant's identifying information against public record databases, fraud and financial institution check databases.
- vii. Reviewing corporate documentation including independent reporting services and, if applicable, documentation on principal owners.
- viii. Visiting the processor's business operations centre.

Financial institutions which provide account services to third-party payment processors should monitor their processor relationships for any significant changes in the processor's business strategies that may affect their risk profile. Financial institutions should periodically re-verify and update the processors' profiles to ensure the risk assessment is appropriate.

In addition to adequate and effective account opening and due diligence procedures for processor accounts, management should monitor these relationships for unusual and suspicious activities. **To effectively monitor these accounts, the financial institution should have an understanding of the following processor information:**

- i. Merchant base.
- ii. Merchant activities.
- iii. Average number of dollar/Naira volume and number of transactions.
- iv. "Swiping" versus "keying" volume for credit card transactions.
- v. Charge-back history, including rates of return for ACH debit transactions and Remotely Created Cheques (RCCs).
- vi. Consumer complaints that suggest a payment processor's merchant clients are inappropriately obtaining personal account information and using it to create unauthorized RCCs or ACH debits.

With respect to account monitoring, a financial institution should thoroughly investigate high levels of returns and should not accept high levels of returns on the basis that the processor has provided collateral or other security to the financial institution. A financial institution should implement appropriate policies, procedures and processes that address compliance and fraud risks. High levels of RCCs or ACH debits returned for insufficient funds or as unauthorized can be an indication of fraud or suspicious activity.

28. OVERVIEW OF PURCHASE AND SALE OF MONETARY INSTRUMENTS

The financial institution's systems should be adequate to manage the risks associated with monetary instrument and the management should have the ability to implement its monitoring and reporting systems effectively.

Monetary instruments are products provided by financial institutions and include cashier's cheques, traveller's cheques, and money orders. Monetary instruments are typically purchased to pay for commercial or personal transactions and, in the case of traveller's cheques, as a form of stored value for future purchases.

Risk Factors

The purchase or exchange of monetary instruments at the placement and layering stages of money laundering can conceal the source of illicit proceeds. As a result, financial institutions have been major targets in laundering operations because they provide and process monetary instruments through deposits. For example, customers or non-customers have been known to purchase monetary instruments in amounts below the reportable currency threshold to avoid having to provide adequate identification. Subsequently, monetary instruments are then placed into deposit accounts to circumvent the CTR filing threshold.

Risk Mitigation

Financial institutions selling monetary instruments should have appropriate policies, procedures and processes in place to mitigate risk. **Policies should define:**

- i. Acceptable and unacceptable monetary instrument transactions (e.g., non-customer transactions, monetary instruments with blank payees, unsigned monetary instruments, identification requirements for structured transactions, or the purchase of multiple sequentially numbered monetary instruments for the same payee).

- ii. Procedures for reviewing for unusual or suspicious activity, including elevating concerns to management.
- iii. Criteria for closing relationships or refusing to do business with non-customers who have consistently or egregiously been involved in suspicious activity.

29. OVERVIEW OF BROKERED DEPOSITS

The financial institution's systems should be adequate to manage the risks associated with brokered deposit relationship and the management should have the ability to implement its due diligence, monitoring and reporting systems effectively.

The use of brokered deposits is a common funding source for many banks and other financial institutions. **Recent technology developments allow brokers to provide bankers with increased access to a broad range of potential investors who have no relationship with the bank and/or other financial institutions. Deposits can be raised over the internet through certificates of deposit listing services or through other advertising methods.**

Deposit brokers provide intermediary services for financial institutions and investors. This activity is considered higher risk because each deposit broker operates under its own guidelines for obtaining deposits. The level of regulatory oversight over deposit brokers varies, as the applicability of AML/CFT Regulatory requirements directly on the deposit broker varies. However, the deposit broker is subject to other statutory requirements regardless of its regulatory status. Consequently, the deposit broker may not be performing adequate customer due diligence. The financial institution accepting brokered deposits depends on the deposit broker to sufficiently perform required account opening procedures and to follow applicable AML/CFT Compliance Program requirements.

Risk Factors

Money laundering and terrorist financing risks arise because the financial institution may not know the ultimate beneficial owners or the source of funds. The deposit broker could represent a range of clients that may be of higher risk for money laundering and terrorist financing (e.g., non-resident or offshore customers, politically exposed persons (PEP) or foreign shell banks).

Risk Mitigation

Financial institutions which accept deposit broker accounts or funds should develop appropriate policies, procedures and processes that establish minimum CDD procedures for all deposit brokers providing deposits to the bank or other financial institution. The level of due diligence performed by a financial institution should be commensurate with its knowledge of the deposit broker and the deposit broker's known business practices and customer base.

In an effort to address the risk inherent in certain deposit broker relationships, financial institutions may want to consider having a signed contract that sets out the roles and responsibilities of each party and restrictions on types of customers (e.g., non-resident or offshore customers, PEPs or foreign shell banks). Financial institutions should conduct sufficient due diligence on deposit brokers, especially unknown, foreign, independent or unregulated deposit brokers. **To manage the ML/FT risks associated with brokered deposits, the financial institution should:**

- i. Determine whether the deposit broker is a legitimate business in all operating locations where the business is conducted.
- ii. Review the deposit broker's business strategies, including targeted customer markets (e.g., foreign or domestic customers) and methods for soliciting clients.
- iii. Determine whether the deposit broker is subject to regulatory oversight.
- iv. Evaluate whether the deposit broker's AML/CFT compliance policies, procedures, and processes are adequate (e.g., ascertain whether the deposit broker performs sufficient CDD including CIP procedures).
- v. Evaluate the adequacy of the deposit broker's AML/CFT audits and ensure that they address compliance with applicable regulations and requirements.

Financial institutions should take particular care in their oversight of deposit brokers who are not adequately regulated entities and:

- i. Are unknown to the financial institution.
- ii. Conduct business or obtain deposits primarily in other jurisdictions.
- iii. Use unknown businesses and financial institutions for references.
- iv. Provide other services that may be suspect, such as creating shell companies for foreign clients.
- v. Refuse to provide requested audit and due diligence information or insist on placing deposits before providing this information.
- vi. Use technology that provides anonymity to customers.

Financial institutions should also monitor existing deposit broker relationships for any significant changes in business strategies that may influence the broker's risk profile. As such, financial institutions should periodically re-verify and update each deposit broker's profile to ensure an appropriate risk assessment.

30. OVERVIEW OF NON-DEPOSIT INVESTMENT PRODUCTS

The financial institution's systems should be adequate to manage the risks associated with both networking and in-house non-deposit investment products (NDIP) and the management should have the ability to implement its monitoring and reporting systems effectively.

NDIP include a wide array of investment products (e.g., securities, bonds and fixed or variable annuities). Sales programs may also include cash management sweep accounts to retail and commercial clients; these programs are offered by the bank directly. Banks and other financial institutions offer these investments to increase fee income and provide customers with additional products and services. The manner in which the NDIP relationship is structured and the methods with which the products are offered substantially affect the bank's/other financial institution's ML/FT risks and responsibilities.

In-House Sales and Proprietary Products

The financial institution is fully responsible for in-house NDIP transactions completed on behalf of its customers either with or without the benefit of an internal broker/dealer employee. In addition, the bank or other financial institution may also offer its own proprietary NDIPs which can be created and offered by the bank or other financial institution, its subsidiary or affiliate.

With in-house sales and proprietary products, the entire customer relationship and all ML/FT risks may need to be managed by the financial institution, depending on how the products are sold.

Financial institution management should assess risk on the basis of a variety of factors such as:

- i. Type of NDIP purchased and the size of the transactions.
- ii. Types and frequency of transactions.
- iii. Country of residence of the principals or beneficiaries, the country of incorporation or the source of funds.

- iv. Accounts and transactions that are not usual and customary for the customer or for the financial institution.

For customers that management considers higher risk for money laundering and terrorist financing, more stringent documentation, verification and transaction monitoring procedures should be established. **EDD may be appropriate in the following situations:**

- i. Financial institution is entering into a relationship with a new customer.
- ii. Non-discretionary accounts have a large asset size or frequent transactions.
- iii. Customer resides in a foreign jurisdiction.
- iv. Customer is a PIC or other corporate structure established in a higher-risk jurisdiction.
- v. Assets or transactions are typical for the customer.
- vi. Investment type, size, assets or transactions are typical for the financial institution.
- vii. International funds transfers are conducted, particularly from offshore funding sources.
- viii. The identities of the principals or beneficiaries in investments or relationships are unknown or cannot be easily determined.
- ix. Politically Exposed persons (PEPs) are parties to any investments or transactions.

Risk Factors

ML/FT risks arise because NDIP can involve complex legal arrangements, large amounts and the rapid movement of funds. NDIP portfolios managed and controlled directly by clients pose a greater money laundering risk than those managed by the bank or other financial services provider. Sophisticated clients may create ownership structures to obscure the ultimate control and ownership of these investments. For example, customers can retain a certain level of anonymity by creating Private Investment Companies (PIC), offshore trusts or other investment entities that hide the customer's ownership or beneficial interest.

Risk Mitigation

Management should develop risk-based policies, procedures and processes that enable the bank/other financial institution to identify unusual account relationships and circumstances, questionable assets and sources of funds and other potential areas of risk (e.g., offshore accounts, agency accounts and unidentified beneficiaries). Management should be alert to situations that need additional review or research.

Networking Arrangements

Before entering into a networking arrangement, financial institutions should conduct an appropriate review of the broker/dealer. The review should include an assessment of

the broker/dealer's financial status, management experience, Securities Dealers status, reputation and ability to fulfil its AML/CFT compliance responsibilities as regards the financial institution's customers. Appropriate due diligence would include a determination that the broker/dealer has adequate policies, procedures and processes in place to enable the broker/dealer meet its legal obligations. The financial institution should maintain documentation on its due diligence of the broker/dealer. Furthermore, detailed written contracts should address the AML/CFT responsibilities, including suspicious activity monitoring and reporting of the broker/dealer and its registered representatives.

A financial institution may also want to mitigate risk exposure by limiting certain investment products offered to its customers. Investment products such as PICs, offshore trusts or offshore hedge funds (may involve international funds transfers) are offered to customers as a way to obscure ownership interests.

Financial institution management should develop and put in place structure that can update due diligence information on the broker/dealer. Such structures should include a periodic review of information on the broker/dealer's compliance with its AML/CFT responsibilities, verification of the broker/dealer's record in meeting testing requirements and a review of consumer complaints. Financial institution management is also encouraged, when possible, to review AML/CFT reports generated by the broker/dealer. This review could include information on account openings, transactions, investment products sold and suspicious activity monitoring and reporting.

31. OVERVIEW OF INSURANCE PRODUCTS

The financial institution's systems should be adequate to manage the risks associated with the sale of covered insurance products and the management should have the ability to implement its monitoring and reporting systems effectively.

Financial institutions engage in insurance sales to increase their profitability, mainly through expanding and diversifying fee-based income. Insurance products are typically sold to financial institution customers through networking arrangements with an affiliate, an operating subsidiary or other third-party insurance providers.

Financial institutions are also interested in providing cross-selling opportunities for customers by expanding the insurance products they offer. Typically, financial institutions take a role as a third-party agent selling covered insurance products. The types of insurance products sold may include life, health, property & casualty, and fixed or variable annuities.

AML/CFT Compliance Programs and Suspicious Transaction Reporting Requirements for Insurance Companies

The insurance regulations apply only to insurance companies, there are no independent obligations for brokers and agents. However, the insurance company is responsible for the conduct and effectiveness of its AML/CFT Compliance Program, which includes agent and broker activities. The insurance regulations only apply to a limited range of products that may pose a higher risk of abuse by money launderers and terrorist financiers. **A covered product for the purposes of an AML/CFT Compliance Program includes:**

- i. A permanent life insurance policy other than a group life insurance policy.
- ii. Any annuity contract other than a group annuity contract.
- iii. Any other insurance product with features of cash value or investment.

When an insurance agent or broker is already required to establish an AML/CFT Compliance Program under a separate requirement of the regulations issued by National Insurance Corporation of Nigeria (NAICOM) (e.g., financial institution or securities broker requirements), the insurance company generally may rely on that Compliance Program to address issues at the time of sale of the covered product. However, the financial institution may need to establish specific policies, procedures and processes for its insurance sales in order to submit information to the insurance company for the insurance company's AML/CFT compliance.

Risk Factors

Insurance products can be used to facilitate money laundering. For example, currency can be used to purchase one or more life insurance policies, which may subsequently and quickly be cancelled by a policyholder (also known as "early surrender") for a penalty. The insurance company refunds the money to the purchaser in the form of a cheque. Insurance policies without cash value or investment features are lower risk, but can be used to launder money or finance terrorism through the submission by a policyholder of inflated or false claims to its insurance carrier, which if paid, would enable the insured to recover a part or all of the originally invested payments. **The other ways insurance products can be used to launder money include:**

- i. Borrowing against the cash surrender value of permanent life insurance policies.
- ii. Selling units in investment-linked products (such as annuities).
- iii. Using insurance proceeds from an early policy surrender to purchase other financial assets.
- iv. Buying policies that allow the transfer of beneficial interests without the knowledge and consent of the issuer (e.g., second-hand endowment and bearer insurance policies).

- v. Purchasing insurance products through unusual methods such as currency or currency equivalents.
- vi. Buying products with insurance termination features without concern for the product's investment performance.

Risk Mitigation

To mitigate money laundering risks the financial institution should adopt policies, procedures and processes that include:

- i. The identification of higher-risk accounts.
- ii. Customer due diligence, including EDD for higher-risk accounts.
- iii. Product design & use, types of services offered and unique aspects or risks of target markets.
- iv. Employee compensation and bonus arrangements that are related to sales.
- v. Monitoring, including the review of early policy terminations and the reporting of unusual and suspicious transactions (e.g., a single, large premium payment, a customer's purchase of a product that appears to fall outside the customer's normal range of financial transactions, early redemptions, multiple transactions, payments to apparently unrelated third parties and collateralized loans).
- vi. Recordkeeping requirements.

32. OVERVIEW OF CONCENTRATION ACCOUNTS

The financial institution's systems should be adequate to manage the AML/CFT risks associated with concentration accounts and the management should have the ability to implement its monitoring and reporting systems effectively.

Concentration accounts are internal accounts established to facilitate the processing and settlement of multiple or individual customer transactions within the financial institution, usually on the same day. These accounts may also be **known as special-use, omnibus, suspense, settlement, intra-day, sweep, or collection accounts.** Concentration accounts are frequently **used to facilitate transactions for private banking, trust & custody accounts, funds transfers and international affiliates.**

Risk Factors

Money laundering risk can arise in concentration accounts if the customer-identifying information such as name, transaction amount and account number are separated from the financial transaction. If separation occurs, the audit trail is lost and accounts may be misused or administered improperly. Financial institution that use concentration

accounts should implement adequate policies, procedures and processes covering the operation and recordkeeping for these accounts. Policies should establish guidelines to identify, measure, monitor and control the risks.

Risk Mitigation

Because of the risks involved, management should be familiar with the nature of their customers' businesses and with the transactions flowing through the financial institution's concentration accounts. Additionally, the monitoring of concentration account transactions is necessary to identify and report unusual or suspicious transactions.

Internal controls are necessary to ensure that processed transactions include the identifying customer information. Retaining complete information is crucial for compliance with regulatory requirements as well as ensuring adequate transaction monitoring. **Adequate internal controls may include:**

- i. Maintaining a comprehensive system that identifies (institution-wide) the general ledger accounts used as concentration accounts, as well as the departments and individuals authorized to use those accounts.
- ii. Requiring dual signatures on general ledger tickets.
- iii. Prohibiting direct customer access to concentration accounts.
- iv. Capturing customer transactions in the customer's account statements.
- v. Prohibiting customer's knowledge of concentration accounts or their ability to direct employees to conduct transactions through the accounts.
- vi. Retaining appropriate transaction and customer identifying information.
- vii. Frequent reconciling of the accounts by an individual who is independent from the transactions.
- viii. Establishing timely discrepancy resolution process.
- ix. Identifying recurring customer names, institution's involvement in trade finance minimizes payment risk to importers and exporters.

The nature of trade finance activities, however, requires the active involvement of multiple parties on both sides of the transaction. In addition to the basic exporter or importer relationship at the center of any particular trade activity, relationships may exist between the exporter and its suppliers and between the importer and its customers.

Both the exporter and importer may also have other banking relationships. Furthermore, many other intermediary financial and non-financial institutions may provide conduits and services to expedite the underlying documents and payment flows associated with trade transactions. Financial institutions can participate in trade financing by, among other things, providing pre-export financing, helping in the collection process, confirming or issuing letters of credit, discounting drafts and

acceptances or offering fee-based services such as providing credit and country information on buyers. Although most trade financing is short-term and self-liquidating in nature, medium-term loans (one to five years) or long-term loans (more than five years) may be used to finance the import and export of capital goods such as machinery and equipment.

In transactions that are covered by letters of credit, financial institutions are required to take the following roles:

Applicant - The buyer or party who requests the issuance of a letter of credit.

Issuing Bank - The bank that issues the letter of credit on behalf of the applicant and advises it to the beneficiary either directly or through an advising financial institution. The applicant is the issuing bank's customer.

Confirming Bank – Typically, is in the home country of the beneficiary and at the request of the issuing bank. It is the financial institution that adds its commitment to honour draws made by the beneficiary, provided the terms and conditions of the letter of credit are met.

Advising Bank - The bank that advises the credit at the request of the issuing bank. The issuing bank sends the original credit to the advising bank for onward forwarding to the beneficiary. The advising bank authenticates the credit and advises it to the beneficiary. There may be more than one advising bank in a letter of credit transaction. The advising bank may also be a confirming bank.

Beneficiary - The seller or party to whom the letter of credit is addressed.

Negotiation - The purchase by the nominated bank of drafts (drawn on a bank other than the nominated bank) or documents under a complying presentation by advancing or agreeing to advance funds to the beneficiary on or before the banking day on which reimbursement is due to the nominated bank.

Nominated Bank - The bank with which the credit is available or any bank in which the credit is available.

Accepting Bank - The bank that accepts a draft, providing a draft is called for by the credit. Drafts are drawn on the accepting bank that dates and signs the instrument.

Discounting Bank - The bank that discounts a draft for the beneficiary after it has been accepted by the accepting bank. The discounting bank is often the accepting bank.

Reimbursing Bank - The bank authorized by the issuing bank to reimburse the paying bank submitting claims under the letter of credit.

Paying Bank - The bank that makes payment to the beneficiary of the letter of credit. As an example, in a letter of credit arrangement, a bank can serve as the issuing bank, allowing its customer (the buyer) to purchase goods locally or internationally, or the bank can act as an advising bank, enabling its customer (the exporter) to sell its goods locally or internationally. The relationship between any two banks may vary and could include any of the roles listed above.

Risk Factors

The international trade system is subject to a wide range of risks and vulnerabilities that provide criminal organizations with the opportunity to launder the proceeds of crime and move funds to terrorist organizations with a relatively low risk of detection. The involvement of **multiple parties on both sides** of any international trade transaction can make the process of due diligence more difficult. Also, because trade finance can **be more document-based than other banking activities, it can be susceptible to documentary fraud** which can be linked to money laundering, terrorist financing or the **circumvention of sanctions or other restrictions** (such as export prohibitions, licensing requirements or controls).

While financial institutions should be alert to transactions involving higher-risk goods (e.g., trade in weapons or nuclear equipment), they need to be aware that goods may be over or undervalued in an effort to evade AML/CFT requirements or customs regulations, or to move funds or value across national borders. For example, an importer may pay a large sum of money from the proceeds of an illegal activity for goods that are essentially worthless and are subsequently discarded. Alternatively, trade documents such as invoices may be fraudulently altered to hide the scheme. Variations on this theme include inaccurate or double invoicing, partial shipment of goods (short shipping) and the use of fictitious goods. Illegal proceeds transferred in such transactions thereby appear sanitized and enter the realm of legitimate commerce. Moreover, many suspect trade finance transactions also involve collusion between buyers and sellers.

The applicant's true identity or ownership may be disguised by the use of certain corporate forms such as shell companies or offshore front companies. The use of these types of entities results in a lack of transparency, effectively hiding the identity of the purchasing party and thus increasing the risk of money laundering and terrorist financing.

Risk Mitigation

Sound CDD procedures are needed to gain a thorough understanding of the customer's underlying business and locations served. The financial institutions in the letter of credit process need to undertake varying degrees of due diligence depending upon their role in the transaction. For example, issuing bank should conduct sufficient due diligence on a prospective customer before establishing the letter of credit. The due diligence should include gathering sufficient information on the applicants and beneficiaries including their identities, nature of business and sources of funding. This may require the use of background checks or investigations, particularly in higher-risk jurisdictions. As such, financial institutions should conduct a thorough review and reasonably know their customers prior to facilitating trade-related activity and should have a thorough understanding of trade finance documentation.

Likewise, guidance provided by the Financial Action Task Force (FATF) on money laundering has helped in setting important industry standards and is a resource for financial institutions that provide trade finance services. The Wolfsberg Group also has published suggested industry standards and guidance for financial institutions that provide trade finance services.

Financial institutions taking other roles in the letter of credit process should complete due diligence that is commensurate with their roles in each transaction. Financial institutions need to be aware that because of the frequency of transactions in which multiple banks are involved, issuing banks may not always have correspondent relationships with the advising or confirming bank.

To the extent feasible, financial institutions should review documentation, not only for compliance with the terms of the letter of credit, but also for anomalies or red flags that could indicate unusual or suspicious transaction. Reliable documentation is critical in identifying potentially suspicious transaction. When analyzing trade transactions for unusual or suspicious transaction, financial institutions should consider obtaining copies of official Nigerian or foreign government import and export forms to assess the reliability of documentation provided. These anomalies could appear in shipping documentation, obvious under or over-invoicing, government licences (when required) or discrepancies in the description of goods on various documents. Identification of these elements may not, in itself, require the filing of STRs, but may suggest the need for further research and verification. In circumstances where STRs are warranted, the financial institution is not expected to stop trade or discontinue processing the transaction. However, stopping the trade may be required to avoid a potential violation of the Money Laundering (Prohibition) Act and its sanctions.

Trade finance transactions frequently use **Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages**. Nigerian financial institutions must comply with relevant regulations and when necessary, provide funding in advance

of consummating the deal involved. Financial institutions should monitor the names of the parties contained in these messages and compare the names against terrorist lists. Financial institutions with a high volume of SWIFT messages should determine whether their monitoring efforts are adequate to detect suspicious transaction, particularly if the monitoring mechanism is not automated.

Policies, procedures and processes should also require a thorough review of all applicable trade documentation (e.g., customs declarations, trade documents, invoices, etc) to enable the financial institution to monitor and report unusual and suspicious transactions based on the role played by the financial institution in the letter of credit process. The sophistication of the documentation review process and MIS should be commensurate with the size and complexity of the financial institution's trade finance portfolio and its role in the letter of credit process. **The monitoring process should give greater scrutiny to:**

- i. Items shipped that are inconsistent with the nature of the customer's business (e.g., a steel company that starts dealing in paper products or an information technology company that starts dealing in bulk pharmaceuticals).
- ii. Customers conducting business in higher-risk jurisdictions.
- iii. Customers shipping items through higher-risk jurisdictions including transit through non-cooperative countries.
- iv. Customers involved in potentially higher-risk activities including activities that may be subject to export/import restrictions (e.g., equipment for military or police organizations of foreign governments, weapons, ammunition, chemical mixtures, classified defense articles, sensitive technical data, nuclear materials, precious gems, or certain natural resources such as metals, ore and crude oil).
- v. Obvious over or under-pricing of goods and services.
- vi. Obvious misrepresentation of quantity or type of goods imported or exported.
- vii. Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction.
- viii. Customer directs payment of proceeds to an unrelated third party.
- ix. Shipment locations or description of goods not consistent with letter of credit.
- x. Significantly amended letters of credit without reasonable justification or changes to the beneficiary or location of payment.

Unless customer behaviour or transaction documentation appears unusual, the financial institution should not be expected to spend undue time or effort reviewing all information. The examples above, particularly for an issuing bank, may be included as part of its routine CDD process. Financial institution with robust CDD programs may find that less focus is needed on individual transactions as a result of their comprehensive knowledge of the customer's activities.

33. OVER VIEW OF PRIVATE BANKING ACTIVITIES

The financial institution's systems should be adequate to manage the risks associated with private banking activities and the management should have the ability to implement its due diligence, monitoring and reporting systems effectively.

Private banking activities are generally defined as providing personalized services to higher net worth customers (e.g., estate planning, financial advice, lending, investment management, bill paying, mail forwarding and maintenance of a residence). Private banking has become an increasingly important business line for large and diverse banking organizations and a source of enhanced fee income.

Nigerian financial institution manage private banking relationships for both domestic and international customers. Typically, thresholds of private banking service are based on the amount of assets for management and on the need for specific products or services (e.g., real estate management, closely held company oversight, money management). **The fees charged are ordinarily based on asset thresholds and the use of specific products and services.**

Private banking arrangements are typically structured to have a central point of contact (i.e., relationship officer/manager) that acts as a liaison between the client and the financial institution and facilitates the client's use of the financial institution's financial services and products.

Typical products and services offered in a private banking relationship include:

- i. Cash management (e.g., cheque-accounts, overdraft privileges, cash sweeps and bill-paying services).
- ii. Funds transfers.
- iii. Asset management (e.g., trust, investment advisory, investment management and custodial and brokerage services).
- iv. The facilitation of shell companies and offshore entities (e.g., Private Investment Companies (PIC), International Business Corporations (IBC) and trusts).
- v. Lending services (e.g., mortgage loans, credit cards, personal loans and letters of credit).
- vi. Financial planning services including tax and estate planning.
- vii. Custody services.
- viii. Other services as requested (e.g., mail services).

Privacy and confidentiality are important elements of private banking relationships. Although customers may choose private banking services simply to manage their assets, they

may also seek a confidential, safe and legal haven for their capital. When acting as a fiduciary, financial institutions have statutory, contractual and ethical obligations to uphold.

Risk Factors

Private banking services can be vulnerable to money laundering schemes and past money laundering prosecutions have demonstrated that vulnerability. **Vulnerabilities to money laundering include the following:**

- i. Private bankers as client advocates.
- ii. Powerful clients including politically exposed persons, industrialists and entertainers.
- iii. Culture of confidentiality and the use of secrecy jurisdictions or shell companies
- iv. Private banking culture of lax internal controls.
- v. Competitive nature of the business.
- vi. Significant profit potential for the financial institution.

Risk Mitigation

Effective policies, procedures and processes can help protect financial institutions from becoming conduits for or victims of money laundering, terrorist financing and other financial crimes that are perpetrated through private banking relationships. Illicit activities through the private banking unit could result in significant financial costs and reputational risk to the financial institution. Financial impacts could include regulatory sanctions and fines, litigation expenses, the loss of business, reduced liquidity, asset seizures and freezes, loan losses and remediation expenses.

Customer Risk Assessment in Private Banking

Financial institutions should assess the risks its private banking activities pose on the basis of the scope of operations and the complexity of the financial institution's customer relationships. Management should establish a risk profile for each customer to be used in prioritizing oversight resources and for ongoing monitoring of relationship activities.

The following factors should be considered when identifying risk characteristics of private banking customers:

- i. Nature of the customer's wealth and the customer's business - The source of the customer's wealth, the nature of the customer's business and the extent to which the customer's business history presents an increased risk for money laundering and terrorist financing. This factor should be considered for private banking accounts opened for politically exposed persons (PEP).

- ii. **Purpose and anticipated activity** - The size, purpose, types of accounts, products and services involved in the relationship, and the anticipated activity of the account.
- iii. **Relationship** - The nature and duration of the financial institution's relationship (including relationships with affiliates) with the private banking customer.
- iv. **Customer's corporate structure** - Type of corporate structure (Private, public, holding, etc).
- v. **Geographic location and jurisdiction** - The geographic location of the private banking customer's domicile and business (domestic or foreign). The review should consider the extent to which the relevant jurisdiction is internationally recognized as presenting a greater risk for money laundering or conversely, is considered to have robust AML/CFT standards.
- vi. **Public information** - Information known or reasonably available to the financial institution about the private banking customer. The scope and depth of this review should depend on the nature of this relationship and the risks involved.

Customer Due Diligence

Customer Due Diligence (CDD) is essential when establishing any customer relationship and it is critical for private banking clients. Financial institutions should take reasonable steps to establish the identity of their private banking clients and as appropriate, the beneficial owners of accounts. Adequate due diligence should vary based on the risk factors identified previously. Policies, procedures and processes should define acceptable CDD for different types of products, services and account holders. As due diligence is an ongoing process, a financial institution should take measures to ensure account profiles are current and monitoring should be risk-based. Financial institutions should consider whether risk profiles should be adjusted or suspicious transaction reported when the activity is inconsistent with the profile.

For purposes of the customer identification program (CIP), the financial institution is not required to search the private banking account to verify the identities of beneficiaries. Instead, it is required to verify the identity of the named account holder only. However, the **CIP rule also provides that** based on the financial institution's risk assessment of a new account opened by a customer that is not an individual (e.g., private banking accounts opened for a PIC), the institution may need "to obtain information about" individuals with authority or control over such an account, including signatories in order to verify the customer's identity to determine whether the account is maintained for non-Nigerians.

Before opening accounts, financial institutions should collect the following information from the private banking clients:

- i. Purpose of the account.
- ii. Type of products and services to be used.
- iii. Anticipated account activity.
- iv. Description and history of the source of the client's wealth.
- v. Client's estimated net worth, including financial statements.
- vi. Current source of funds for the account.
- vii. References or other information to confirm the reputation of the client.

Bearer Shares of Shell Companies

Some shell companies issue bearer shares. **Bearer shares allow their ownership to be vested on their bearer and the ownership of the company to therefore be conveyed by simply transferring of the physical possession of the shares.** Risk mitigation of shell companies that issue bearer shares may include maintaining control of the bearer shares, entrusting the shares with a reliable independent third party or requiring periodic certification of ownership. Financial institutions should assess the risks these relationships pose and determine the appropriate controls. For example, in most cases, financial institutions should choose to maintain (or have an independent third party maintain) bearer shares for their customers. In rare cases that involve lower-risk, well-known, long-time customers, financial institutions may find that periodically re-certifying of the beneficial ownership is effective. A strong CDD program is an effective underlying control through which financial institutions can determine the nature, purpose and expected use of shell companies and apply appropriate monitoring and documentation standards.

Board of Directors and Senior Management Oversight of Private Banking Activities

The board of directors' and senior management's active oversight of private banking activities and the creation of an appropriate corporate governance oversight culture are crucial elements of a sound risk management and control environment. **The purpose and objectives of the institution's private banking activities should be clearly identified and communicated by the board and senior management.** Well-developed goals and objectives should describe the target client base in terms of minimum net worth, investable assets, types of products and services sought. Goals and objectives should also specifically describe the types of clients the financial institution will and will not accept and should establish appropriate levels of authorization for new-client acceptance. Board and senior management should also be actively involved in establishing control and risk management goals for private banking activities, including effective audit and compliance reviews. Each financial institution should ensure that its policies, procedures and processes for conducting private banking activities are evaluated and updated regularly and ensure that roles, responsibilities and accountability are clearly delineated.

Employee compensation plans are often based on the number of new accounts established or on an increase in the managed assets. Board and senior management should ensure that compensation plans do not create incentives for employees to ignore appropriate due diligence and account opening procedures or possible suspicious activity relating to the account. Procedures that require various levels of approval for accepting new private banking accounts can minimize such opportunities.

Given the sensitive nature of private banking and the potential liability associated with it, financial institutions should thoroughly investigate the background of newly hired private banking relationship managers. During the course of employment, any indications of inappropriate activities should be promptly investigated by the financial institution.

Additionally, when private banking relationship managers change employers, their customers often move with them. Financial institutions bear the same potential liability for the existing customers of newly hired officers as they do for any new, private banking relationship. Therefore, those accounts should be promptly reviewed using the financial institution's procedures for establishing new account relationships.

MIS and reports are also important in effectively supervising and managing private banking relationships and risks. Board and senior management should review relationship manager compensation reports, budget or target comparison reports and applicable risk management reports. Private banker MIS reports should enable the relationship manager to view and manage the whole client and any related client relationships.

34. OVERVIEW OF TRUST AND ASSET MANAGEMENT SERVICES

Objective

The financial institution's policies, procedures, processes and systems to manage the ML/FT risks associated with trust and asset management services should be adequate and the management should have the ability to implement effective due diligence, monitoring and reporting systems effectively.

Trust accounts are generally defined as a legal arrangement in which one party (the trustor or grantor) transfers ownership of assets to a person or bank/other financial institution (the trustee) to be held or used for the benefit of others. These arrangements include the broad categories of court-supervised accounts (e.g., executorships and guardianships), personal trusts (e.g.,

living trusts, trusts established under a will, charitable trusts) and corporate trusts (e.g., bond trusteeships).

Agency accounts are established by contract and governed by contract law.

Assets are held under the terms of the contract and legal title or ownership does not transfer to the financial institution as agent. **Agency accounts include custody, escrow, investment management and safekeeping relationships.** Agency products and services may be offered in a traditional trust department or through other financial institution departments.

Customer Identification Program

Customer identification program (CIP) rules apply to all financial institutions' accounts. **The CIP rule defines an "account" to include cash management, safekeeping, and custodian and trust relationships but excludes employee benefit accounts.**

For purposes of the CIP, the financial institution is not required to search the trust, escrow or similar accounts to verify the identities of beneficiaries. Instead, it is required to verify the identity of the named accountholder (the trust) only. In the case of a trust account, the customer is the trust whether or not the financial institution is the trustee for the trust. However, the CIP rule also provides that, based on the financial institution's ML/FT risk assessment of a new account opened by a customer that is not an individual, the financial institution may need "to obtain information about" individuals with authority or control over such an account, including the signatories in order to verify the customer's identity.

For example, in certain circumstances involving revocable trusts, the financial institution may need to gather information about the settlor, grantor, trustee, or other persons with the authority to direct the trustee and who thus have authority or control over the account in order to establish the true identity of the customer.

In the case of an escrow account, if a financial institution establishes an account in the name of a third party such as a real estate agent (who is acting as agent) then, the financial institution's customer is the escrow agent.

If the financial institution is the escrow agent, then the person who establishes the account is the financial institution's customer. For example, if the purchaser of real estate directly opens an escrow account and deposits funds to be paid to the seller upon satisfaction of specified conditions, the financial institution's customer will be the purchaser. Further, if a company in formation establishes an escrow account for investors to deposit their subscriptions pending receipt of a required minimum amount, the financial institution's customer will be the company in formation (or if not yet a legal entity, the person opening the account on its behalf).

However, the CIP rule also provides that, based on the financial institution's ML/FT risk assessment of a new account opened by a customer that is not an individual, the financial institution may need "to obtain information about" individuals with authority or control over such an account including the signatories in order to verify the customer's identity.

ML/FT Risk Factors

Trust and asset management accounts including agency relationships present ML/FT concerns similar to those of deposit taking, lending and other traditional financial institution's activities. Concerns are primarily due to the unique relationship structures involved when the financial institution handles trust and agency activities, such as:

- i. Personal and court-supervised accounts.
- ii. Trust accounts formed in the private banking department.
- iii. Asset management and investment advisory accounts.
- iv. Global and domestic custody accounts.
- v. Securities lending.
- vi. Employee benefit and retirement accounts.
- vii. Corporate trust accounts.

Transfer Agent Accounts

- i. Other related business lines.

As in any account relationship, money laundering risk may arise from trust and asset management activities. When misused, trust and asset management accounts can conceal the sources and uses of funds as well as the identity of beneficial and legal owners. Customers and account beneficiaries may try to remain anonymous in order to move illicit funds or avoid scrutiny.

For example, customers may seek a certain level of anonymity by creating private investment companies offshore trusts or other investment entities that hide the true ownership or beneficial interest of the trust.

Risk Mitigation

Management should develop policies, procedures and processes that enable the financial institution to identify unusual account relationships & circumstances, questionable assets & sources of assets and other potential areas of ML/FT risk (e.g., offshore accounts, PICs, asset protection trusts (APT), agency accounts and unidentified beneficiaries). While the majority of traditional trust and asset management accounts will not need EDD, management should be alert to those situations that need additional review or research.

Customer Comparison Against Various Lists

The financial institution must maintain required CIP information and complete the required one-time check of trust account names against VIS search requests. The financial institution should also be able to identify customers who may be politically exposed persons (PEP), doing business with or located in a jurisdiction designated as "primary money laundering concern. The financial institution should also determine the identity of other parties that may have control over the account, such as grantors or co-trustees.

Circumstances Warranting Enhanced Due Diligence

i. Management should assess account risk on the basis of a variety of factors which may include:

- a. Type of trust or agency account and its size.
- b. Types and frequency of transactions.
- c. Country of residence of the principals or beneficiaries or the country where established or source of funds.
- d. Accounts and transactions that are not usual and customary for the customer or for the financial institution.
- e. Stringent documentation, verification and transaction monitoring procedures should be established for accounts that the management considers as higher risk. Typically, employee benefit accounts and court-supervised accounts are among the lowest ML/FT risks.

ii. Circumstance in which EDD may be appropriate:

The financial institution is entering into a relationship with a new customer.

- a. Account principals or beneficiaries reside in a foreign jurisdiction or the trust or its funding mechanisms are established offshore.
- b. Assets or transactions are not typical for the type and character of the customer.
- c. Account type, size, assets or transactions are atypical for the financial institution.
- d. International funds transfers are conducted particularly through offshore funding sources.
- e. Accounts are funded with easily transportable assets such as gemstones, precious metals, coins, artwork, rare stamps or negotiable instruments.
- f. Accounts or relationships are maintained in way that the identities of the principals, beneficiaries, sources of funds are unknown or cannot be easily determined.
- g. Accounts transactions are for the benefit of charitable organizations or other non-governmental organizations (NGOs) that may be used as a conduit for illegal activities.

- h. Interest on lawyers' trust accounts (IOLTA) holding are processing significant currency/dollar amounts.
- i. Account assets that include PICs.
- j. PEPs are parties to the accounts or transactions.

35. OVERVIEW OF EXPANDED EXAMINATION AND PROCEDURES FOR PERSONS AND ENTITIES

Overview of Non-resident Aliens and Foreign Individuals

The financial institution's systems to manage the risks associated with transactions involving accounts held by non-resident aliens (NRA) and foreign individuals should be adequate and the management should have the ability to implement its due diligence, monitoring and reporting systems effectively.

Foreign individuals maintaining relationships with Nigerian financial institutions can be divided into two categories of **resident aliens and non-resident aliens**.

For definitional purposes, a NRA is a non-Nigerian citizen who: (i) is not a lawful permanent resident of Nigeria during the calendar year and who does not meet the substantial presence test or (ii) has not been issued an alien registration permit. The FIRS determines the tax liabilities of a foreign person and officially defines the person as a "resident" or "non-resident."

Although NRAs are not permanent residents, they may have a legitimate need to establish an account relationship with a Nigerian financial institution. NRAs can use bank products and services for asset preservation (e.g., mitigating losses due to exchange rates), business expansion and investments.

Risk Factors of NRA Account Holder

Financial institutions may find it more difficult to verify and authenticate an NRA account holder's identification, source of funds and source of wealth which may result in ML/FT risks. The NRA's home country may also heighten the account risk, depending on the secrecy laws of that country. Because the NRA is expected to reside outside of Nigeria, funds transfers or the use of foreign automated teller machines (ATM) may be more frequent. The ML/FT risk may be further heightened if the NRA is a politically exposed person (PEP).

Risk Mitigation

Financial institutions should establish policies, procedures and processes that provide for sound due diligence and verification practices, adequate risk assessment

of NRA accounts, ongoing monitoring and reporting of unusual or suspicious activities. **The following factors are to be considered when determining the risk level of an NRA account:**

- i. Account-holder's home country.
- ii. Types of products and services used.
- iii. Forms of identification.
- iv. Source of wealth and funds.
- v. Unusual account activity.

The financial institution's CIP should detail the identification requirements for opening an account for a non-Nigerian person, including a NRA. The program should include the use of documentary and non-documentary methods to verify a customer. In addition, financial institutions must maintain due diligence procedures for private banking accounts for non-Nigerian persons, including those held for PEPs or senior foreign political figures.

36. OVERVIEW OF POLITICALLY EXPOSED PERSONS

The financial institution's systems to manage the risks associated with senior local/foreign political figures, often referred to as "politically exposed persons" (PEP) should be adequate and the management should have the ability to implement its risk-based due diligence, monitoring and reporting systems effectively.

Financial institution should take all reasonable steps to ensure that they do not knowingly or unwittingly assist in hiding or moving the proceeds of corruption by senior local/foreign political figures, their families and associates. Because the risks presented by PEPs will vary by customer, product, service, country and industry, identifying, monitoring and designing controls for these accounts and transactions should be risk-based.

The term "politically exposed persons" generally include individuals who are or have been entrusted with prominent public functions in Nigeria and/or foreign countries and people/entities associated with them. **As specified in the CBN AML/CFT Regulation 2009, examples of PEPs include but not limited to:**

- i. Heads of State or government;
- ii. State Governors;
- iii. Local Government Chairmen;
- iv. Senior Politicians;
- v. Senior government officials;
- vi. Judicial or military officials;
- vii. Senior executives of state owned corporations;

- viii. Important political party officials;
- ix. Family members or close associates of PEPs; and
- x. Members of Royal Families.

In addition to performing CDD measures, financial institutions are required to put in place appropriate risk management systems and procedures that include reasonable steps to determine and ascertain whether a potential customer or existing customer or the beneficial-owner is a politically exposed person. Risk will vary depending on other factors such as products and services used and size or complexity of the account relationship. **Financial institutions also should consider various factors when determining if an individual is a PEP, including:**

- i. Official responsibilities of the individual's office.
- ii. Nature of the title (e.g., honorary or salaried).
- iii. Level and nature of authority or influence over government activities or other officials.
- iv. Access to significant government assets or funds.

Financial institutions are also required to obtain senior management approval before they establish business relationships with a PEP and to render monthly returns on all their transactions with PEPs to the CBN (**refer to pages B1402 – B1403 of the CBN AML/CFT Regulation 2009, for guidance**).

In determining the acceptability of higher-risk accounts, a financial institution should be able to obtain sufficient information to determine whether an individual is or is not a PEP. For example, when conducting due diligence on a higher-risk account, it would be usual for a financial institution to review a customer's income sources, financial information and professional background. These factors would likely require some review of past and present employment as well as general references that may identify a customer's status as a PEP. Moreover, a financial institution should always keep in mind that identification of a customer's status as a PEP should not automatically result in a higher-risk determination. **It is not only one factor that the institution should consider in assessing the risk of such a relationship.**

Ascertaining whether a customer has a close association with a senior local/foreign political figure could be difficult. Moreover, focusing on the relationships that are "widely and publicly known" may also provide a reasonable limitation on expectation to identify close associates of PEPs. However, financial institution that has actual knowledge of close associations of its customer should consider such a customer as PEP, even if such association is not otherwise widely or publicly known. Financial institutions are expected to follow reasonable steps to ascertain the status of an individual. The regulatory agencies recognize that these steps may not uncover all close associations of PEPs.

Risk Factors

In high-profile cases over the past few years, PEPs have used financial institutions as conduits for their illegal activities, including corruption, bribery and money laundering. However, not all PEPs present the same level of risk. This risk will vary depending on numerous factors, including the PEP's geographic location, industry, sector, position and level or nature of influence or authority. Risk may also vary depending on factors such as the purpose of the account, the actual or anticipated activity, products and services used, and size or complexity of the account relationship.

As a result of these factors, some PEPs may be of lower risk and some may be of higher risk for local/foreign corruption or money laundering. Financial institutions that conduct business with dishonest PEPs face substantial reputational risk, additional regulatory scrutiny and possible supervisory action. Financial institution also should be alert to a PEP's access to, control of or influence over government or corporate accounts; the level of involvement of intermediaries, vendors, suppliers, and agents in the industry or sector in which the PEP operates; and the improper use of corporate vehicles and other legal entities to obscure ownership.

Risk Mitigation

Section 1.10.5 of the CBN AML/CFT Regulation 2009, requires "financial institutions to take reasonable measures to establish the source of wealth and the source of funds of customers and beneficial owners identified as PEPs". Financial institutions should exercise reasonable judgment in designing and implementing policies, procedures and processes regarding PEPs. Financial institution should obtain risk-based due diligence information on PEPs and establish policies, procedures and processes that provide for appropriate scrutiny and monitoring. It is critical and in order to have appropriate risk-based account opening procedures for big ticket transaction or higher-risk products and services. The opening of an account is the prime opportunity for the financial institution to gather information for all customers, including PEPs. **Commensurate with the identified level of risk, due diligence procedures should include, but are not necessarily limited to, the following:**

- i. Identify the account-holder and beneficial owner, including the nominal and beneficial owners of companies, trusts, partnerships, private investment companies, or other legal entities that are accountholders.
- ii. Seek information directly from the account holder and beneficial owner regarding possible PEP status.

- iii. Identify the account holder's and beneficial owner's country (ies) of residence and the level of risk for corruption and money laundering associated with these jurisdictions.
- iv. Obtain information regarding employment including industry and sector, and the level of risk for corruption associated with the industries and sectors.
- v. Check references (as appropriate) to determine whether the account holder and beneficial owner is or has been a PEP.
- vi. Identify the account holder's and beneficial owner's source of wealth and funds.
- vii. Obtain information on immediate family members or close associates that have the account.
- viii. Determine the purpose of the account, the expected volume and nature of account activity.
- ix. Make reasonable efforts to review public sources of information. These sources will vary depending upon each situation. However, financial institutions should check the account-holder and any beneficial owners of legal entities against reasonably accessible public sources of information (e.g., government databases, major news publications, commercial databases and other databases available on the internet, as appropriate).

PEP accounts are not limited to large or internationally focused financial institutions. **A PEP can open an account at any financial institution, regardless of its size or location.** Financial institutions should have risk-based procedures for identifying PEP accounts and assessing the degree of risks involved and the latter will vary. **Senior management should be involved in the decision to accept a PEP account. If management determines after-the-fact that an account is a PEP account, it should evaluate the risks and take appropriate steps. The financial institution should exercise additional, reasonable due diligence with regard to such accounts.**

For example, the financial institution may increase reference inquiries, obtain additional background information on the PEP from branches or correspondents operating in the client's home country, and make reasonable efforts to consult publicly available information sources. **On-going risk-based monitoring of PEP accounts is critical to ensuring that the accounts are being used as anticipated.**

37. OVERVIEW OF EMBASSY AND FOREIGN CONSULATE ACCOUNTS

The financial institution's systems to manage the risks associated with transactions involving embassy and foreign consulate accounts should be adequate and the

management should have the ability to implement its due diligence, monitoring and reporting systems effectively.

Embassies contain the offices of the foreign ambassador, the diplomatic representative and their staff. The embassy, led by the ambassador, is a foreign government's official representation in the Nigeria (or other country).

Foreign consulate offices act as branches of the embassy and perform various administrative and governmental functions (e.g., issuing visas and handling immigration matters). Foreign consulate offices are typically located in major metropolitan areas. In addition, foreign ambassadors' diplomatic representatives, their families and associates may be considered politically exposed persons (PEP) in certain circumstances.

Embassies and foreign consulates in Nigeria require access to the banking system to meet many of their day-to-day financial responsibilities. Such services can range from account relationships for operational expenses (e.g., payroll, rent and utilities) to inter and intra-governmental transactions (e.g., commercial and military purchases). In addition to official embassy accounts, some financial institutions provide ancillary services or accounts to embassy staff, families and current or prior foreign government officials. Each of these relationships poses different levels of risk to the financial institution.

Embassy accounts, including those accounts for a specific embassy office such as a cultural or education ministry, a defence attaché or ministry, or any other account should have a specific operating purpose, stating the official function of the foreign government office. Consistent with established practices for business relationships, these embassy accounts should have written authorization by the foreign government.

Risk Factors

To provide embassy and foreign consulate services, **a Nigerian financial institution may need to maintain a foreign correspondent relationship with the embassy's or foreign consulate's financial institution.** Financial institutions conducting business with foreign embassies or consulates should assess and understand the potential risks of these accounts and should develop appropriate policies, procedures and processes. **Embassy or foreign consulate accounts may pose a higher risk in the following circumstances:**

- i. Accounts are from countries that have been designated as higher risk.
- ii. Substantial currency transactions take place in the accounts.
- iii. Account activity is not consistent with the purpose of the account (e.g., pouch activity or payable upon proper identification transactions).
- iv. Accounts directly fund personal expenses of foreign nationals including but not limited to expenses for college students.

- v. Official embassy business is conducted through personal accounts.

Risk Mitigation

Financial institutions should obtain comprehensive due diligence information on embassy and foreign consulate account relationships. For private banking accounts for non-Nigerian persons specifically, financial institutions must obtain due diligence information. The financial institution's due diligence related to embassy and foreign consulate account relationships should be commensurate with the risk levels presented. In addition, financial institutions are expected to establish policies, procedures and processes that provide for greater scrutiny and monitoring of all embassy and foreign consulate account relationships. Management should fully understand the purpose of the account and the expected volume and nature of account activity. On-going monitoring of embassy and foreign consulate account relationships is critical to ensuring that the account relationships are being used as anticipated.

38. OVERVIEW OF DESIGNATED NON-FINANCIAL INSTITUTIONS

The financial institution's systems to manage the risks associated with accounts of designated non- financial institutions (DNFI) should be adequate and the management should have the ability to implement its monitoring and reporting systems effectively.

Common examples of NBFIs include but not limited to:

- i. Casinos, hotels, supermarkets and card clubs.
- ii. Dealers in cars, luxury goods, chartered accountants, audit firms, clearing and settlement companies, legal practitioners.
- iii. Dealers in precious metals, stones or jewellery.

Some NBFIs are currently required to develop an AML/CFT program, comply with the reporting and recordkeeping requirements of the MLPA, and report suspicious activity to Federal Ministry of Commerce as the regulatory authority. DNFI typically need access to banking services in order to operate. While financial institutions are expected to manage risk associated with all accounts including DNFI accounts, the institution will not be held responsible for their customers' non-compliance with the MLPA and other relevant laws and regulations.

Risk Factors

DNFI industries are extremely diverse, ranging from large multi-national corporations to small, independent businesses that offer financial services only as an ancillary component to their primary business (e.g., grocery store that offers cheque-cashing). The range of products and services offered and the customer bases served by DNFI are equally diverse. As a result of this diversity, some DNFI may be of lower risk and some may be of higher risk for money laundering. **Financial institutions that maintain account relationships with DNFI may be exposed to a higher risk for potential money laundering activities because many DNFI:**

- i. Lack ongoing customer relationships and require minimal or no identification by customers.
- ii. Maintain limited or inconsistent record-keeping on customers and transactions. Ma
- iii. Engage in frequent currency transactions. E
- iv. Be subject to varying levels of regulatory requirements and oversight. Ar
- v. Can quickly change their product mix or location and quickly enter or exit an operation. Ca
- vi. Sometimes operate without proper registration or licensing. So

Risk Mitigation

Financial institutions that maintain account relationships with DNFI should develop policies, procedures and processes to:

- i. Identify DNFI relationships. Id
- ii. Assess the potential risks posed by the DNFI relationships. As
- iii. Conduct adequate and ongoing due diligence on the DNFI relationships when necessary. Co
- iv. Ensure DNFI relationships are appropriately considered within the financial institution’s suspicious activity monitoring and reporting systems. iv

Risk assessment factors of financial institutions assess the risks posed by their DNFI customers and direct their resources most appropriately to those accounts that pose a more significant money laundering risk.

Risk factors may be used to help identify the relative risks within the DNFI portfolio. Nevertheless, management should weigh and evaluate each risk assessment factor to arrive at a risk determination for each customer and to prioritize oversight resources. **Relevant risk factors include:**

- i. Types of products and services offered by the DNFI.
- ii. Locations and markets served by the DNFI.
- iii. Anticipated account activity.
- iv. Purpose of the account.

A financial institution's due diligence should be commensurate with the level of risk of the DNFI customer identified through its risk assessment. If a financial institution's risk assessment indicates potential for a heightened risk of money laundering or terrorist financing, it will be expected to conduct further due diligence in a manner commensurate with the heightened risk.

Providing Banking Services to Money Services Businesses

Money Services Businesses (MSBs) are subject to the full range of MLPA regulatory requirements, including the anti-money laundering program rule, suspicious activity and currency transaction reporting rules and various other identification and record-keeping rules.

The following regulatory expectations apply to financial institution with MSB customers:

- i. The MLPA does not require financial institutions to serve as the de facto regulator of any type of DNFI industry or individual DNFI customer, including MSBs.
- ii. While financial institutions are expected to manage risk associated with all accounts including MSB accounts, they will not be held responsible for the MSB not having AML/CFT Program.
- iii. Not all MSBs pose the same level of risk and not all MSBs will require the same level of due diligence. Accordingly, if a financial institution's assessment of the risks of a particular MSB relationship indicates a lower risk of money laundering or other illicit activity, a financial institution is not routinely expected to perform further due diligence (such as reviewing information about an MSB's AML/CFT Program) beyond the minimum due diligence expectations. Unless indicated by the risk assessment of the MSB, financial institutions are not expected to routinely review an MSB's AML/CFT Program.

MSB Risk Assessment

An effective risk assessment should be a composite of multiple factors and depending upon the circumstances, certain factors may be given more weight than others. **The following factors may be used to help identify the level of risk presented by each MSB customer:**

- i. Purpose of the account.
- ii. Anticipated account activity (type and volume).
- iii. Types of products and services offered by the MSB.
- iv. Locations and markets served by the MSB.

Financial institution management may tailor these factors based on their customer base or the geographic locations in which the financial institution operates. Management should weigh and evaluate each risk assessment factor to arrive at a risk determination for each customer. A bank's due diligence should be commensurate with the level of risk assigned to the MSB customer, after consideration of these factors. If a bank's risk assessment indicates potential for a heightened risk of money laundering or terrorist financing, the bank will be expected to conduct further due diligence in a manner commensurate with the heightened risk.

MSB Risk Mitigation

A financial institution's policies, procedures and processes should provide for sound due diligence and verification practices, adequate risk assessment of MSB accounts and ongoing monitoring and reporting of unusual or suspicious transactions. A financial institution that establishes and maintains accounts for MSBs should apply appropriate, specific risk-based and where necessary, EDD policies, procedures, and controls.

The factors below, while not all inclusive may reduce or mitigate the risk in some MSB accounts:

- i. MSB is registered and licensed with the CBN.
- ii. MSB confirms it is subject to examination for AML compliance.
- iii. MSB affirms the existence of a written AML/CFT Program and provides its CCO's name and contact information.
- iv. MSB has an established banking relationship and/or account activity consistent with expectations.
- v. MSB is an established business with an operating history.
- vi. MSB is a principal with one or few agents, or is acting as an agent for one principal.
- vii. MSB provides services only to local residents.
- viii. Most of the MSB's customers conduct routine transactions in not too much amounts.

- ix. The expected (lower-risk) transaction activity for the MSB's business operations is consistent with information obtained by the financial institution at account opening. **Examples include the following:**
 - a. Cheque-cashing activity is limited to payroll or government cheques;
 - b. Cheque-cashing service is not offered for third-party or out-of-state cheques.
- x. Money-transmitting activities are limited to domestic entities (e.g., domestic bill payments).

MSB Due Diligence Expectations

Given the importance of licensing and registration requirements, a financial institution should file a STR if it becomes aware that a customer is operating in violation of the registration or licensing requirements. **The decision to maintain or close an account should be made by financial institution senior management under standards and guidelines approved by its board of directors.**

The extent to which the financial institution should perform further due diligence beyond the minimum due diligence obligations set forth below will be dictated by the level of risk posed by the individual MSB customer. Because not all MSBs present the same level of risk, not all MSBs will require further due diligence. For example, a local grocer that also cashes payroll cheques for customers purchasing groceries may not present the same level of risk as a money transmitter specializing in cross-border funds transfers. Therefore, the customer due diligence requirements will differ based on the risk posed by each MSB customer. **Based on existing AML/CFT Regulation requirements applicable to financial institutions, the minimum due diligence expectations associated with opening and maintaining accounts for any MSB are:**

- i. Apply the financial institution's CIP.
- ii. Confirm registration renewal.
- iii. Confirm compliance with licensing requirements, if applicable.
- iv. Confirm agent status, if applicable.
- v. Conduct a basic ML/FT risk assessment to determine the level of risk associated with the account and whether further due diligence is necessary.

If the institution determines that the MSB customer presents a higher level of money laundering or terrorist financing risk, EDD measures should be conducted in addition to the minimum due diligence procedures. **Depending on the level of perceived risk, the size and sophistication of the particular MSB, banking organizations may pursue some or all of the following actions as part of an appropriate EDD review:**

- i. Review the MSB's AML/CFT Program.
- ii. Review results of the MSB's independent testing of its AMLCFT Program.
- iii. Review written procedures for the operation of the MSB.
- iv. Conduct on-site visits.
- v. Review list of agents, including locations within or outside Nigeria which will be receiving services directly or indirectly through the MSB account.
- vi. Review written agent management and termination practices for the MSB.
- vii. Review written employee screening practices for the MSB.

39. OVERVIEW OF PROFESSIONAL SERVICE PROVIDERS

The financial institution's systems to manage the risks associated with professional service provider relationships should be adequate and the management should have the ability to implement its due diligence, monitoring and reporting systems effectively.

A professional service provider acts as an intermediary between its client and the financial institution. Professional service providers include lawyers, accountants, investment brokers and other third parties that act as financial liaisons for their clients. These providers may conduct financial dealings for their clients. For example, an attorney may perform services for a client or arrange for services to be performed on the client's behalf. Such services include settlement of real estate transactions, asset transfers, management of client monies, investment services and trust arrangements.

Risk Factors

In contrast to escrow accounts that are set up to serve individual clients, professional service provider accounts allow for ongoing business transactions with multiple clients. Generally, a financial institution has no direct relationship with or knowledge of the beneficial owners of these accounts who may be a constantly changing group of individuals and legal entities.

As with any account that presents third-party risk, the financial institution could be more vulnerable to potential money laundering abuse. **Some potential examples of abuse could include:**

- i. Laundering illicit currency.
- ii. Structuring currency deposits and withdrawals.
- iii. Opening any third-party account for the primary purpose of masking the underlying client's identity.

As such, the financial institution should establish an effective due diligence program for the professional service provider.

Risk Mitigation

When establishing and maintaining relationships with professional service providers, financial institutions should adequately assess account risk and monitor the relationship for suspicious or unusual activity. At account opening, the financial institution should have an understanding of the intended use of the account, including anticipated transaction volume, products and services used, and geographic locations involved in the relationship.

40. OVERVIEW OF NON-GOVERNMENTAL ORGANIZATIONS AND CHARITIES

The financial institution's systems to manage the risks associated with accounts of non-governmental organizations (NGO) should be adequate and charities and the management should have the ability to implement its due diligence, monitoring and reporting systems effectively.

NGOs are private non-profit organizations that pursue activities intended to serve the public good. NGOs may provide basic social services work to relieve suffering, promote the interests of the poor, bring citizen concerns to governments, encourage political participation, protect the environment, or undertake community development to serve the needs of citizens, organizations or groups in one or more of the communities that the NGO operates. An NGO can be any non-profit organization that is independent from government.

NGOs can range from large regional, national or international charities to community-based self-help groups. NGOs may also include research institutes, churches, professional associations and lobby groups. NGOs typically depend (in whole or in part) on charitable donations and voluntary service for support.

Risk Factors

Because NGOs can be used to obtain funds for charitable organizations, the flow of funds both into and out of the NGO can be complex, making them susceptible to abuse by money launderers and terrorists. Guidelines will be issued to assist charities in adopting practices to reduce the risk of terrorist financing or abuse.

Risk Mitigation

To assess the risk of NGO customers, a financial institution should conduct adequate due diligence on the organization. **In addition to required CIP information, due diligence for NGOs should focus on other aspects of the organization, such as the following:**

- i. Purpose and objectives of their stated activities.
- ii. Geographic locations served including headquarters and operational areas.
- iii. Organizational structure.
- i. Donor and volunteer base.
- ii. Funding and disbursement criteria including basic beneficiary information.
- iii. Record keeping requirements.
- iv. Its affiliation with other NGOs, governments or groups.
- v. Internal controls and audits.

For accounts that financial institution management considers to be higher risk, stringent documentation, verification and transaction monitoring procedures should be established. NGO accounts that are at higher risk for ML/FT concerns include those operating or providing services internationally, conducting unusual or suspicious activities or lacking proper documentation. **EDD for these accounts should include:**

- i. Evaluating the principals.
- ii. Obtaining and reviewing the financial statements and audits.
- iii. Verifying the source and use of funds.
- iv. Evaluating large contributors or grantors to the NGO.

41. OVERVIEW OF BUSINESS ENTITIES (DOMESTIC AND FOREIGN)

The financial institution's systems to manage the risks associated with transactions involving domestic and foreign business entities should be adequate and the management should have the ability to implement its due diligence, monitoring and reporting systems effectively.

The term "business entities" refers to limited liability companies, corporations, trusts, and other entities that may be used for many purposes such as tax and estate planning. Business entities are relatively easy to establish. Individuals, partnerships and existing corporations establish business entities for legitimate reasons but the entities may be abused for money laundering and terrorist financing.

Domestic Business Entities

Nigeria has statutes governing the incorporation and operation of business entities, including limited liability companies, corporations, general partnerships, limited partnerships and trusts.

Shell companies registered in Nigeria are a type of domestic business entity that may pose heightened risks. Shell companies can be used for money laundering and other crimes because they are easy and inexpensive to form and operate. In addition, ownership and transactional information can be concealed from regulatory agencies and law enforcement in large part because it requires minimal disclosures of such information during the formation process.

The term “domestic” refers to entities formed or organized in Nigeria. These entities may have no other connection to Nigeria and ownership and management of the entities may reside abroad.

The term “shell company” generally refers to an entity without a physical presence in any country.

Shares of shell companies can be publicly traded or privately held. Although publicly traded shell companies can be used for illicit purposes, the vulnerability of the shell company is compounded when it is privately held and beneficial ownership can more easily be obscured or hidden. Lack of transparency of beneficial ownership can be a desirable characteristic for some legitimate uses of shell companies, but it is also a serious vulnerability that can make some shell companies ideal vehicles for money laundering and other illicit financial activity. In some, only minimal information is required to register articles of incorporation or to establish and maintain “good standing” for business entities — increasing the potential for their abuse by criminal and terrorist organizations.

Foreign Business Entities

Frequently used foreign entities include trusts, investment funds and insurance companies. **Two foreign entities that can pose particular money laundering risk are International Business Corporations (IBC) and Private Investment Companies (PIC) opened in Offshore Financial Centres (OFCs).** Many OFCs have limited organizational disclosure and record-keeping requirements for establishing foreign business entities, creating an opportune environment for money laundering.

International Business Corporations

IBCs are entities formed outside of a person’s country of residence which can be used to maintain confidentially or hide assets. IBC ownership can, based on jurisdiction, be conveyed through registered or bearer shares. **There are a variety of advantages to using an IBC which include, but are not limited to, the following:**

- i. Asset protection.
- ii. Estate planning.

- iii. Privacy and confidentiality.
- iv. Reduction of tax liability.

Through an IBC, an individual is able to conduct the following:

- i. Open and hold bank accounts.
- ii. Hold and transfer funds.
- iii. Engage in international business and other related transactions.
- iv. Hold and manage offshore investments (e.g., stocks, bonds, mutual funds and certificates of deposit) many of which may not be available to “individuals” depending on their location of residence.
- v. Hold corporate debit and credit cards, thereby allowing convenient access to funds.

Private Investment Companies

PICs are separate legal entities. They are essentially subsets of IBCs. Determining whether a foreign corporation is a PIC is based on identifying the purpose and use of the legal vehicle. **PICs are typically used to hold individual funds and investments, and ownership can be vested through bearer shares or registered shares.** Like IBCs, PICs can offer confidentiality of ownership, hold assets centrally and may provide intermediaries between private banking customers and the potential beneficiaries of the PICs. Shares of a PIC may be held by a trust, which further obscures beneficial ownership of the underlying assets. **IBCs, including PICs, are incorporated frequently in countries that impose low or no taxes on company assets and operations or are bank secrecy havens.**

Risk Factors

Money laundering and terrorist financing risks arise because business entities can hide the true owner of assets or property derived from or associated with criminal activity. The privacy and confidentiality surrounding some business entities may be exploited by criminals, money launderers and terrorists. Verifying the grantors and beneficial owner(s) of some business entities may be extremely difficult, as the characteristics of these entities shield the legal identity of the owner. Few public records will disclose true ownership. Overall, the lack of ownership transparency; minimal or no record-keeping requirements, financial disclosures and supervision; and the range of permissible activities all increase money laundering risk.

While business entities can be established in most international jurisdictions, many are incorporated in OFCs that provide ownership privacy and impose few or no tax obligations. To maintain anonymity, many business entities are formed with nominee directors, office-holders and shareholders. In certain jurisdictions, business entities can also be established using bearer shares; ownership records are not maintained, rather

ownership is based on physical possession of the stock certificates. Revocable trusts are another method used to insulate the grantor and beneficial owner and can be designed to own and manage the business entity, presenting significant barriers to law enforcement.

The following indicators of potentially suspicious activity may be commonly associated with shell company activity

- i. Insufficient or no information available to positively identify originators or beneficiaries of funds transfers (using internet, commercial database searches or direct inquiries to a respondent bank).
- ii. Payments have no stated purpose, do not reference goods or services. They identify only a contract or invoice number.
- iii. Goods or services, if identified, do not match profile of company provided by respondent bank or character of the financial activity; a company references remarkably dissimilar goods and services in related funds transfers; explanation given by foreign respondent bank is inconsistent with observed funds transfer activity.
- iv. Transacting businesses share the same address, provide only a registered agent's address or other inconsistent addresses.
- v. Many or all of the funds transfers are sent in large, round amounts.
- vi. Unusually large number and variety of beneficiaries receiving funds transfers from one company.
- vii. Frequent involvement of multiple jurisdictions or beneficiaries located in higher-risk OFCs.
- viii. A foreign correspondent bank exceeds the expected volume in its client profile for funds transfers, or an individual company exhibits a high volume and pattern of funds transfers that is inconsistent with its normal business activity.
- ix. Multiple high-value payments or transfers between shell companies with no apparent legitimate business purpose.
- vi. Purpose of the shell company is unknown or unclear.

Risk Mitigation

Management should develop policies, procedures and processes that enable the financial institution to identify account relationships in particular deposit accounts, with business entities and monitor the risks associated with these accounts in all the financial institution's departments. Business entity customers may open accounts within the private banking department, within the trust department, or at local branches. Management should establish appropriate due diligence at account opening and during the life of the relationship to manage risk in these accounts. The financial institution should gather sufficient information on the business entities and their beneficial owners to understand and assess the risks of the account relationship. Important information for determining the valid use of these entities includes the type of business, the

purpose of the account, the source of funds and the source of wealth of the owner or beneficial owner.

The financial institution's CIP should detail the identification requirements for opening an account for a business entity. When opening an account for a customer that is not an individual, financial institution should obtain information about the individuals who have authority and control over such accounts in order to verify the customer's identity (the customer being the business entity). Required account opening information may include articles of incorporation, a corporate resolution by the directors authorizing the opening of the account, or the appointment of a person to act as a signatory for the entity on the account. Particular attention should be paid to articles of association that allow for nominee shareholders, board members and bearer shares.

If the financial institution, through its trust or private banking departments, is facilitating the establishment of a business entity for a new or existing customer, the money laundering risk to the financial statement is typically mitigated. Because the financial institution is aware of the parties (e.g., grantors, beneficiaries and shareholders) involved in the business entity, initial due diligence and verification is easier to obtain. Furthermore, in such cases, the financial institution frequently has ongoing relationships with the customers initiating the establishment of a business entity.

Risk assessments may include a review of the domestic or international jurisdiction where the business entity was established, the type of account (or accounts) and expected versus actual transaction activities, the types of products that will be used, and whether the business entity was created in-house or externally. If ownership is held in bearer share form, financial institution should assess the risks these relationships pose and determine the appropriate controls. In most cases, financial institutions should choose to maintain (or have an independent third party maintain) bearer shares for customers. In rare cases involving lower-risk, well-known, established customers, financial institutions may find that periodically re-certifying beneficial ownership is effective. The financial institution's risk assessment of a business entity customer becomes more important in complex corporate formations. For example, a foreign IBC may establish a series of layered business entities with each entity naming its parent as its beneficiary.

On-going account monitoring is critical to ensure that the accounts are reviewed for unusual and suspicious activity. The financial institution should be aware of higher-risk transactions in these accounts, such as activity that has no business or apparent lawful purpose, funds transfer activity to and from higher-risk jurisdictions, currency intensive transactions and frequent changes in the ownership or control of the non-public business entity.

42. OVERVIEW OF CASH-INTENSIVE BUSINESSES

The financial institution's systems to manage the risks associated with cash-intensive businesses and entities should be adequate and the management should have the ability to implement its due diligence, monitoring and reporting systems effectively.

Cash-intensive businesses and entities cover various industry sectors. Most of these outfits conduct legitimate business. However, some aspects of these businesses may be susceptible to money laundering or terrorist financing. **Common examples include but are not limited to, the following:**

- i. Convenience stores.
- ii. Restaurants.
- iii. Retail stores.
- iv. iv Liquor stores.
- v. Cigarette distributors.
- vi. Privately owned automated teller machines (ATM).
- vii. Vending machine operators.
- viii. Parking garages.

Risk Factors

Some businesses and entities may be misused by money launderers to legitimize their illicit proceeds. For example, a criminal may own a cash-intensive business such as a restaurant and use it to launder currency from illicit criminal activities. The restaurant's currency deposits with its bank do not, on the surface, appear unusual because the business is legitimately a cash-generating entity. However, the volume of currency in a restaurant used to launder money will most likely be higher in comparison with similar restaurants in the area. The nature of cash-intensive businesses and the difficulty in identifying unusual activity may cause these businesses to be considered higher risk.

Risk Mitigation

When establishing and maintaining relationships with cash-intensive businesses, financial institution should establish policies, procedures and processes to identify higher-risk relationships; assess ML/FT risks; complete due diligence at account opening and periodically throughout the relationship; and include such relationships in appropriate monitoring for unusual or suspicious activity. At the time of account opening, the financial institution should have an understanding of the customer's business operations; the intended use of the account including anticipated transaction volume, products and services used; and the geographic locations involved in the relationship.

When conducting a risk assessment of cash-intensive businesses, financial institution should direct their resources to those accounts that pose the greatest risk of money laundering or terrorist financing. **The following factors may be used to identify the risks:**

- i. Purpose of the account.
- ii. Volume, frequency and nature of currency transactions.
- iii. Customer history (e.g., length of relationship, CTR and STR filings).
- iv. Primary business activity, products and services offered.
- v. Business or business structure.
- vi. Geographic locations and jurisdictions of operations.
- vii. Availability of information and cooperation of the business in providing information. For those customers deemed to be particularly higher risk management may consider implementing sound practices such as periodic on-site visits, interviews with the business's management or closer reviews of transactional activity.