



Central Bank of Kenya

**Prudential Guideline on Anti-Money Laundering, Combating
the Financing of Terrorism and Proliferation Financing
CBK/PG/08**

August 2026

TABLE OF CONTENTS

PART I: PRELIMINARY

- 1.1 Title
- 1.2 Application
- 1.3 Authorisation
- 1.4 Definitions

PART II: STATEMENT OF POLICY

- 2.1 Purpose
- 2.2 Scope
- 2.3 Responsibility

PART III: BACKGROUND

- 3.1 What is Money Laundering?
- 3.2 What is Terrorism Financing
- 3.3 What is Proliferation Financing?
- 3.4 International Standard Setters

PART IV: KENYA'S AML/CFT/CPF LEGAL AND REGULATORY FRAMEWORK

PART V: SPECIFIC REQUIREMENTS

- 5.1 Specific Measures
- 5.2 Application of the Risk-Based Approach
- 5.3 The AML/CFT/CPF Governance Framework
- 5.4 The AML/CFT/CPF Compliance Program
- 5.5 Customer Due Diligence
- 5.6 Ongoing Due Diligence
- 5.7 Enhanced Customer Due Diligence Measures
- 5.8 Simplified Due Diligence Measures
- 5.9 Non-Face-To-Face Verification
- 5.10 Reliance on Third Parties
- 5.11 Failure to Complete CDD Measures
- 5.12 Politically Exposed Persons (PEPs)
- 5.13 Correspondent Banking
- 5.14 Prohibition on Shell Banks
- 5.15 Higher Risk Countries

- 5.16 Wire Transfers
- 5.17 Money Value or Transfer Services
- 5.18 New Technologies
- 5.19 Suspicious Transactions Reports
- 5.20 Tipping Off
- 5.21 Cash Transaction Reports
- 5.22 The Cross Border Conveyance of Monetary Instruments
- 5.23 Record Keeping

PART VI: TARGETED FINANCIAL SANCTIONS

- 6.1 Definitions
- 6.2 Introduction
- 6.3 Targeted Financial Sanctions Related to Terrorism Financing
- 6.4 Targeted Financial Sanctions Related to Proliferation Financing
- 6.5 Policies, Procedures and Systems
- 6.6 Sanctions List
- 6.7 The Consolidated List
- 6.8 Designation and Circulation of Sanctions lists International UNSCRs Regimes
- 6.9 Designation and Circulation of Sanction List - UNSCR 1373 (Domestic List)
- 6.10 Obligations of Financial Institutions upon Receipt of Sanctions List
- 6.11 Prohibition on Making Frozen Funds Available to Designated Person or Entities
- 6.12 False Positives
- 6.13 Delisting
- 6.14 Authorisation to Access Funds or Other Assets Subject to Freezing Measures
- 6.15 Third Party Claims
- 6.16 Reporting Obligations
- 6.17 Record Keeping - Targeted Financial Sanctions
- 6.18 Ongoing Sanctions Screening and Monitoring
- 6.19 United Nations Security Council Resolutions Sanctions Regimes Arising from Threats to International Peace and Security

PART VII: SPECIAL CONSIDERATIONS FOR INSTITUTIONS THAT ONBOARD VIRTUAL ASSET SERVICE PROVIDERS

- 7.1 Introduction
- 7.2 Areas of Consideration
- 7.3 Applicable Laws and Regulations
- 7.4 Specific Measures

PART VIII: REMEDIAL MEASURES

PART IX: EFFECTIVE DATE

9.1 Effective Date

9.2 Supersedence

PART X: ENQUIRIES

ACRONYMS

AML	Anti-Money Laundering
BO	Beneficial Owner
BRS	Business Registration Service
CDD	Customer Due Diligence
CBK	Central Bank of Kenya
CBR	Correspondent Banking Relationship
CFT	Combating the Financing of Terrorism
CFTIMC	The Counter Financing of Terrorism Inter-Ministerial Committee
CPF	Combating Proliferation Financing
EDD	Enhanced Due Diligence
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
FATF	Financial Action Taskforce
FRC	Financial Reporting Centre
KRA	Kenya Revenue Authority
IPRS	Integrated Population Registration System
ML	Money Laundering
MVTS	Money Value or Transfer Service
PEP	Politically Exposed Person
PF	Proliferation Financing
PF Regulations	The Prevention of Terrorism (Implementation of United Nations Security Council Resolutions on Prevention Suppression and Disruption of Proliferation Financing) Regulations
POCAMLA	The Proceeds of Crime and Anti-Money Laundering Act
POTA	The Prevention of Terrorism Act
POCAML Regulations	The Proceeds of Crime and Anti-Money Laundering Regulations
RBA	Risk-Based Approach
SDD	Simplified Due Diligence
STR	Suspicious Transaction Report
TF	Terrorism Financing
TF Regulations	The Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on Suppression Terrorism Regulations
TFS	Targeted Financial Sanctions
UNSCR	United Nations Security Council Resolution
VASP	Virtual Asset Service Provider
VASP Regulations	Virtual Asset Service Providers Regulations 2026

PART I: PRELIMINARY

- 1.1 Title** – This Guideline shall be cited as the Guideline on Anti-Money Laundering, Combating the Financing of Terrorism and Proliferation Financing
- 1.2 Application** – All institutions licensed under the Banking Act (Cap.488) and their foreign branches and subsidiaries.
- 1.3 Authorisation** – This Guideline is issued pursuant to Section 33(4) of the Banking Act, which empowers the Central Bank of Kenya (CBK) to issue guidelines to institutions for the purpose of maintaining a stable and efficient banking and financial system and Section 33D(2) (g) of the Banking Act, which authorises the Central Bank of Kenya to issue guidelines on anti-money laundering, combating the financing of terrorism and proliferation financing (AML/CFT/CPF).

1.4 Definitions

“beneficial owner” means a natural person who ultimately owns or controls a customer or the natural person on whose behalf a transaction is being conducted and includes any natural person who ultimately exercises effective control over a legal person or arrangement.

A **“business relationship”** is any arrangement between the institution and a customer the purpose of which is to facilitate the carrying out of transactions between the parties on a frequent, habitual or regular basis, and where the monetary value of dealings in the course of the arrangement is not known or capable of being ascertained at the outset. The opening of an account with an institution should therefore be treated as forming a ‘business relationship’.

“competent authorities” means designated government, statutory, regulatory, or investigative bodies that are legally empowered to supervise, regulate, enforce, investigate, or ensure compliance with laws and regulations relating to anti-money laundering, combating the financing of terrorism, and countering proliferation financing.

A **“correspondent banking relationship”** is an arrangement where one bank, the (“correspondent bank”) provides banking services to another bank (the “respondent bank”). Respondent banks may be provided with a wide range of services, including cash management, interest-bearing accounts in a variety of currencies, international wire transfers, cheque clearing, payable-through accounts and foreign exchange services.

“customer” in relation to a transaction or an account, includes:

- (a) natural person, legal person or legal arrangement in whose name a transaction or account is arranged, opened or undertaken;
- (b) signatory to a transaction or account;
- (c) any natural person, legal person or legal arrangement to whom a transaction has been assigned or transferred;
- (d) any natural person, legal person or legal arrangement who is authorised to conduct a transaction;

A **“financial intelligence unit”** is a national centre for receiving, analysing, and disseminating information concerning money laundering, associated predicate offenses, and terrorist financing and proliferation financing. Kenya’s financial intelligence unit is referred to as the Financial Reporting Centre or (FRC).

“know your customer” requirements consist of obtaining full particulars of the customer’s identity (which may need to be verified in certain circumstances) and a sound knowledge of the purpose for which the customer is seeking to establish a business relationship with an institution. This knowledge needs to be applied to all dealings initiated by the customer.

“legal arrangements” means express trusts or other similar legal arrangements.

“legal persons” means any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, partnerships, or associations and other relevantly similar entities.

“monetary instruments” means:

- (a) coins and paper currency designated as legal tender of Kenya or of a foreign country and which is customarily used and accepted as a medium of exchange in Kenya or the country of issue;
- (b) travellers' cheques, personal cheques, bank cheques, money orders or securities;
- (c) any other negotiable instrument which is in bearer form, or other form through which title passes upon delivery;

“money laundering” means the act of a person who:

- (a) engages, directly or indirectly, in a transaction that involves proceeds of any unlawful activity;
- (b) acquires, receives, possesses, disguises, transfers, converts, exchanges, carries,

- (c) disposes, uses, removes from or brings into Kenya proceeds of any unlawful activity; or
- (d) conceals, disguises or impedes the establishment of the true nature, origin, location, movement, deposition, title of, rights with respect to, or ownership of, proceeds of any unlawful activity where:
 - (i) as may be inferred from objective factual circumstances, the person knows; or
 - (ii) has reason to believe that the property is proceeds from any unlawful activity, or in respect of the conduct of a natural person, the person without reasonable excuse fails to take reasonable steps to ascertain whether or not the property is proceeds from any unlawful activity.

“money or value transfer services” means a financial service that involves the acceptance of cash, cheques, other monetary instruments or other stores of value in one location and the payment of a corresponding sum in cash or other form to a beneficiary in another location by means of a communication, message, transfer, or through a clearing network to which the money or value transfer services provider belongs.

A **“occasional transaction”** means any transaction carried out other than in the course of a business relationship. For example, a single foreign currency transaction by a customer who does not have an account at the concerned institution constitutes an occasional transaction.

“person” means any natural or legal entity.

“proceeds of crime” means any property or economic advantage derived or realized, directly or indirectly, as a result of or in connection with an offence irrespective of the identity of the offender and includes, on a proportional basis, property into which any property derived or realized directly from the offence was later successively converted, transformed or intermingled, as well as income, capital or other economic gains derived or realized from such property from the time the offence was committed.

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

“shell bank” means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

“targeted financial sanctions” means both asset freezing and prohibitions to prevent funds or other assets from being made available, directly or indirectly, for the benefit of designated persons and entities.

“terrorism financing” means any act or omission that constitutes the offence of financing terrorism under the Prevention of Terrorism Act, including:

- (a) the direct or indirect collection, provision, attempt to provide, or making available of funds, property or services, where a person knows, intends, or has reasonable grounds to believe that such funds, property or services will be used:
 - (i) to carry out or facilitate the commission of a terrorist act by a terrorist group for any purpose; or
 - (ii) by any individual or group involved in the planning, preparation, execution, participation in, or support of terrorist acts;
- (b) participation, contribution, organisation, direction, or facilitation of the activities described in paragraph (a), including where such contribution is intentional or made with knowledge of the group’s terrorist purpose;
- (c) financing of travel of individuals to a State other than their State of residence or nationality for the purpose of perpetrating, planning, preparing, participating in, or receiving terrorist training.

A **“virtual asset”** means a digital representation of value that can be digitally traded or transferred and can be used for payment or investment purposes and does not include digital representation of fiat currencies, securities and other financial assets.

A **“virtual asset service provider”** means a company licensed under the Virtual Asset Services Providers Act to carry on the business of virtual asset services

“virtual services” means services and activities listed under the First Schedule of the Virtual Assets Service Providers Act. This includes virtual asset wallet providers, virtual asset exchanges, virtual asset payment processors, virtual asset investment advisors, virtual asset managers, virtual asset brokers and virtual asset offerings providers.

A **“wire transfer”** is any transaction carried out on behalf of an originator (natural or legal person) through a financial institution by electronic means, aimed at making funds available to a beneficiary at another financial institution. This applies regardless of whether the sender and recipient are the same.

PART II: STATEMENT OF POLICY

- 2.1 Purpose** - The purpose of this Guideline is to provide guidance regarding the prevention, detection and the control of possible money laundering, terrorism financing or proliferation financing.
- 2.2 Scope** - This Guideline shall apply to all institutions licensed to transact business under the Banking Act. It sets out requirements on preventive measures, including customer due diligence (CDD), record-keeping, the reporting of suspicious transactions, as well as compliance with targeted financial sanctions. It also requires institutions to adopt a risk-based approach to ensure that measures to manage and mitigate money laundering, terrorism financing and proliferation financing (ML/TF/PF) risks are proportionate to the level of risk identified.
- 2.2.1 Applicability** - this Guideline is also applicable to the foreign branches and subsidiaries of institutions licensed to transact business under the Banking Act.
- 2.3 Responsibility** - It is the responsibility of the Board of Directors and senior management of an institution to establish appropriate policies on anti-money laundering and combating the financing of terrorism and proliferation financing (AML/CFT/CPF) procedures and to train staff to ensure adequate identification of customers, source of funds and the use of the said funds. Such policies should also ensure the effective prevention, detection and control of possible money laundering, terrorism financing and proliferation financing.

PART III: BACKGROUND

3.1 What is Money Laundering?

Money laundering is the process by which criminals conceal or disguise the illegal origin, ownership or control of property or assets that are the proceeds of criminal activity to make them appear to have originated from legitimate sources. If successful, money laundering enables criminals to retain control of the proceeds of crime and to use or dispose of those proceeds without attracting suspicion.

Money laundering is a global phenomenon that affects all countries and financial systems. Preventing the laundering of criminal proceeds is essential to protecting the integrity of the financial system and depriving criminals of the benefits of their unlawful activities.

3.1.1 Money Laundering Predicate Offences

A money laundering predicate offence is the underlying criminal activity that generates proceeds which, when laundered, constitute the offence of money laundering. Predicate offences include, but are not limited to, fraud, corruption, bribery, tax offences, drug trafficking, human trafficking, robbery, insider trading, counterfeiting, environmental crimes, cybercrime and other offences prescribed under applicable laws.

3.1.2 The Need to Combat Money Laundering

The ability to launder the proceeds of crime through the financial system is fundamental to the success of criminal enterprises. Criminals rely on financial institutions and other businesses to disguise the origin of illicit proceeds and integrate them into the legitimate economy.

Financial institutions that fail to implement effective AML measures expose themselves to legal, regulatory, operational, and reputational risks, undermine confidence in the financial system, and may facilitate further criminal activity. Effective AML measures therefore protect both individual institutions and the integrity of Kenya's financial sector

3.2 What is Terrorism Financing?

Terrorism financing is the provision, collection or movement of funds or other assets, by any means, directly or indirectly, with the intention or knowledge that they will be used, in whole or in part, to carry out a terrorist act, support a terrorist organisation, or facilitate terrorist activities.

Unlike money laundering, the funds used to finance terrorism may originate from either lawful or unlawful sources. Financial institutions should therefore remain vigilant to transactions that may facilitate terrorism financing regardless of the source of the funds.

3.2.1 The Need to Combat Terrorism Financing

Terrorism financing poses a significant threat to national security, public safety, and the stability of the financial system. It diverts financial resources from legitimate economic activity and may be used to support terrorist acts both within and outside Kenya.

Financial institutions play a critical role in identifying, preventing, and reporting activities that may be linked to terrorism financing through effective CDD, transaction monitoring, targeted financial sanctions, and the reporting of suspicious transactions.

3.3 What is Proliferation Financing?

Proliferation financing refers to the provision of funds or financial services used, in whole or in part, for the manufacture, acquisition, possession, development, export, transfer, brokering, transport, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery, in contravention of applicable national laws or international obligations.

3.3.1 The Need to Counter Proliferation Financing

Proliferation financing has emerged as a significant threat to international peace and security. Financial institutions may be exposed to proliferation financing risks through trade finance, cross-border payments, correspondent banking relationships, complex corporate structures, and transactions involving sanctioned jurisdictions or dual-use goods.

Financial institutions should implement appropriate measures to identify, assess, understand and mitigate proliferation financing risks, including effective CDD, transaction monitoring, and compliance with targeted financial sanctions.

For additional information on money laundering, terrorism financing and proliferation financing vulnerabilities refer to **Annex I**.

3.4 International Standard Setters

Kenya's AML/CFT/CPF framework is informed by international standards developed by the United Nations (UN), the Financial Action Task Force (FATF) and the Basel Committee on Banking Supervision.

3.4.1 The United Nations

The United Nations provides the international legal framework for combating money laundering, terrorism financing and proliferation financing through international conventions and binding United Nations Security Council Resolutions. These include measures relating to the criminalisation of money laundering and terrorism financing, international cooperation, and the implementation of targeted financial sanctions. Kenya is a party to the relevant international UNSCRs and has implemented these obligations through its domestic legislative and regulatory framework.

Key conventions and UNCRs that Kenya is party to include:

- **The United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention) and the United Nations Convention against Transnational Organized Crime (Palermo Convention)**, which establish measures to combat money laundering and promote international cooperation.
- **The International Convention for the Suppression of the Financing of Terrorism**, which requires the criminalisation and prevention of terrorism financing.
- **UNSCRs 1267/1988, 1373, 1988, 1989 and 2253** relating to targeted financial sanctions against terrorism and terrorist financing.
- **UNSCRs 1718 and 2231** relating to proliferation financing.

3.4.2 The Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) is the international standard-setting body responsible for developing and promoting measures to combat money laundering, terrorist financing and proliferation financing through the FATF Recommendations. Kenya is a member of the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG), the FATF-style regional body for Eastern and Southern Africa. Through its membership,

Kenya is committed to strengthening its AML/CFT/CPF framework in line with the FATF Recommendations and other applicable international standards. This includes developing and strengthening its legal, regulatory and institutional measures to prevent and combat money laundering, terrorist financing and proliferation financing, and participating in mutual evaluations and follow-up processes. Mutual evaluation is a peer review mechanism that assess both the extent to which a country has implemented the FATF Recommendations and the effectiveness of its AML/CFT/CPF framework.

3.4.3 The Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision (BCBS) develops international standards and supervisory guidance for the regulation and supervision of banks. Basel Core Principle 29 (BCP 29) on the abuse of financial services emphasises robust, risk-based CDD and effective compliance functions to prevent banks from being used for criminal activities,

PART IV: KENYA'S AML/CFT/CPF LEGAL FRAMEWORK

Institutions shall comply with the following AML/CFT/CPF laws, regulations:

- (a) **The Proceeds of Crime and Anti-Money Laundering Act (POCAML):** Establishes the legal framework for preventing, detecting, investigating, and prosecuting money laundering. It requires institutions to implement AML/CFT/CPF preventive measures, including conducting CDD maintaining records, reporting suspicious transactions, and implementing appropriate internal controls.
- (b) **The Prevention of Terrorism Act (POTA):** Provides measures for preventing and suppressing terrorism and terrorist financing. It requires institutions to implement controls to detect, report, and freeze funds and other assets linked to terrorism or terrorist financing in accordance with national law and applicable United Nations Security Council resolutions.
- (c) **The Proceeds of Crime and Anti-Money Laundering Regulations:** Prescribe the requirements for implementing POCAML, including customer identification and verification, record-keeping, transaction monitoring, and reporting obligations.
- (d) **The Prevention of Terrorism (Implementation of United Nations Security Council Resolutions on the Suppression of Terrorism) Regulations:** Provide for the implementation of United Nations Security Council resolutions relating to terrorism, including targeted financial sanctions, asset freezing, and reporting obligations.
- (e) **The Prevention of Terrorism (Implementation of United Nations Security Council Resolutions on the Prevention, Suppression, and Disruption of Proliferation Financing) Regulations:** Establish measures for implementing targeted financial sanctions relating to proliferation financing and ensuring compliance with applicable United Nations Security Council resolutions concerning weapons of mass destruction.
- (f) **Other AML/CFT/CPF Guidance:** Institutions shall comply with all applicable AML/CFT/CPF guidelines, directives, circulars and notices issued by CBK and the Financial Reporting Centre (FRC).

PART V: SPECIFIC REQUIREMENTS

5.1 Specific Measures: The Board of Directors of an institution operating in shall ensure that management:

- (a) Establishes adequate internal control measures to address potential money laundering and terrorist financing and proliferation financing risks.
- (b) Obtains, verifies and maintains proper identification of customers wishing to open accounts or make transactions whether directly or through proxy.
- (c) Obtains and maintains adequate records such as; copies or records of official identification documents like passports, identity cards; driving

licenses or similar documents; statements of accounts, account files and business correspondence including the results of any inquiries to establish the background and purpose of any complex, unusual large transactions, for a minimum of seven years, regarding the sources of funds and details of transactions in order to:

- i. Enable the identification of unusual or suspicious transactions.
 - ii. Reconstruct individual transactions.
- (d) Train staff on a regular basis in the prevention, detection and control of money laundering, terrorism financing proliferation financing and the identification of suspicious transactions.
 - (e) Monitor and report any suspicious transactions or activities to the FRC that may indicate money laundering, terrorism financing proliferation financing or other attempts to conceal the true identity of customers or ownership of assets.
 - (f) Cooperate with national law enforcement agencies by taking appropriate measures which are consistent with the law where there are reasonable grounds for suspecting money laundering.
 - (g) While taking into account the sensitive nature of extra-territorial anti-money laundering laws and regulations, ensure that their overseas branches and subsidiaries are aware of the reporting requirements as directed by the Central Bank of Kenya with regard to suspicious transaction reporting and sanctions reporting.

5.2 Application of the Risk-Based Approach

Institutions shall apply a risk-based approach to ensure that mitigation measures applied are proportionate to the level of ML/TF/PF risks identified and commensurate with the nature, scale, and complexity of an institution's operations.

For an in-depth are advised to refer to the AML/CFT/CPF Risk Management Guidelines.

5.2.1 ML/TF/PF Risk Assessments

Institutions shall:

- (a) Undertake a ML/TF/PF risk assessments to identify, assess, understand, monitor, manage, and mitigate their ML/TF/PF risks.
- (b) In undertaking their risk assessments, institutions shall:

- (i) Document the risk assessment.
- (ii) Consider all relevant risk factors, including:
 - customers;
 - countries/geographical areas;
 - products and services;
 - delivery channels; and
 - any other risk factors relevant to the institution's business.
- (iii) Review and update the ML/TF/PF risk assessment at least every two years, or earlier where there are material changes so that the assessment remains current. Examples of material changes that would make it necessary to update risk assessments include:
 - i. Emerging ML/TF/PF risks as identified in updates to the National Risk Assessment (NRA) as well as typologies reports on emerging ML/TF/PF trends and methods.
 - ii. Outcomes of sectoral ML/TF/PF risk assessments conducted by CBK.
 - iii. The enactment or amendment of AML/CFT/CPF laws, regulations, or supervisory guidance.
 - iv. Changes in senior management or governance structures of an institution.
 - v. Structural changes affecting an institution's risk profile, such as mergers or acquisitions.
 - vi. Changes in an institution's business strategy including products and services offered, and customer profile.
- (c) Ensure that the ML/TF/PF risk assessments and related information are available to CBK, the FRC and other relevant competent authorities upon request.
- (d) Develop, implement, and maintain Board-approved policies, procedures, and controls to manage and mitigate the ML/TF/PF risks identified through the risk assessments.
- (e) Monitor the effectiveness of the policies, procedures, and controls and strengthen them where necessary.
- (f) Submit the ML/TF/PF risk assessment to the CBK annually. This should not be interpreted to mean that institutions update their AML/CFT/CPF risk assessments annually, only when there material changes highlighted under 5.2.1(b) (iii).

5.2.2 Risk

For the purposes of this Guideline, risk refers to the possibility that threats related to

ML/TF/PF may exploit vulnerabilities associated with an institution, resulting in adverse consequences for the institution, the financial system, the economy, or national security. When assessing ML/TF/PF risks, an institution shall consider the interaction of the following components:

(a) Threat

A threat refers to any person, group, object, activity, or circumstance with the potential to engage in, facilitate, or support money laundering, terrorist financing, or proliferation financing.

Threats may arise from, among others:

- i. criminal actors and organised criminal groups;
- ii. terrorist organisations and terrorist financiers;
- iii. proliferators and proliferation financing networks;
- iv. sanctioned persons, entities, or jurisdictions;
- v. predicate offences generating illicit proceeds; and
- vi. emerging typologies, methods, and trends associated with ML, TF or PF activities.

(b) Vulnerability

A vulnerability refers to any weakness, characteristic, deficiency, or exposure that may be exploited by a threat or that may facilitate money laundering, terrorist financing, or proliferation financing.

Vulnerabilities may arise from, among others:

- i. customer types and customer relationships;
- ii. products, services, and business activities;
- iii. delivery channels and distribution mechanisms;
- iv. transaction characteristics;
- v. geographic exposure; and
- vi. deficiencies in governance, internal controls, systems, processes, or oversight arrangements.

(c) Consequence

A consequence refers to the actual or potential impact arising from the occurrence of money laundering, terrorist financing, or proliferation financing activities. Such consequences may include:

- i. financial loss;
- ii. legal or regulatory sanctions;
- iii. reputational damage;
- iv. operational disruption;
- v. loss of confidence in the institution or financial sector; and
- vi. adverse effects on the integrity, stability, and security of the financial system and the broader economy.

5.2.2.1 Risk Assessment Process

Institutions shall implement a structured process for conducting the risk assessment where risk is defined by three factors; threats, vulnerabilities and consequences that:

- (a) Identifies and assesses inherent risk, that is the level of ML/TF/PF risk in the absence of controls, across customers, products, services, transactions, delivery channels, geographic areas, and other relevant factors.
- (b) Analyses the identified risks to determine their potential impact and likelihood.
- (c) Considers residual risk, the level of ML/TF/PF risk remaining after the application of controls, including internal policies, procedures, and mitigation measures.
- (d) Assigns risk ratings to customers, transactions, or business areas to prioritize higher-risk areas.
- (e) Documents the methodology, findings, risk ratings, and mitigation measures to ensure transparency and accountability.

5.2.2.2 Risk Categories

In undertaking a risk assessment, institutions shall amongst others take into account the following risk categories:

(a) Country or Geographic Risk

Institutions should identify domestic and international geographic locations that may pose a higher risk to its AML/CFT compliance program. Each case should be evaluated individually when assessing the risks associated with doing business, such as opening accounts or facilitating transactions, in certain geographic locations.

- i) Factors that may indicate elevated domestic geographic risk include:
 - i. Areas with a high concentration of cash-intensive businesses.
 - ii. Proximity to international borders, seaports, or airports.
 - iii. Ltd. presence of regulated financial institutions.

- iv. Concentrations of higher-risk industries.
 - v. High levels of organised crime or corruption.
- ii) Factors that may result in a foreign country posing a higher risk include:
- i. Countries identified by credible sources as providing funding or support for terrorist activities or that have designated terrorist organisations operating within them.
 - ii. Countries with weak AML/CFT/CPF legal, institutional and supervisory frameworks.
 - iii. Countries characterised by bank secrecy or Ltd. transparency.
 - iv. Countries that are tax havens.
Countries characterised by high levels of organised crime or corruption and trans-national crime.

(b) Products and Services Risk

Institutions shall assess ML/TF/PF risks associated with products and services prior to their introduction and on an ongoing basis and shall ensure that appropriate controls are implemented to mitigate identified risks.

Products and services that may present higher ML/TF/PF risks include, but are not Ltd. to:

- i. funds transfer services;
- ii. electronic money and stored value products;
- iii. domestic and cross-border payment services, including PUPID transactions and third-party payment processors;
- iv. remittance services;
- v. Automated Clearing House (ACH) transactions;
- vi. Teller Machines (ATMs);
- vii. mobile financial services;
- viii. internet and electronic banking services;
- ix. foreign exchange services;
- x. private banking services;
- xi. trust and asset management services;
- xii. monetary instruments;
- xiii. correspondent banking relationships, including payable-through accounts (PTAs);
- xiv. lending activities, particularly those secured by cash collateral or marketable securities;
- xv. safety deposit boxes;

- xvi. virtual asset service providers, including custodial wallet services; virtual asset exchanges, and token offerings; and
- xvi. peer-to-peer lending (P2P) lending , a method of financing that allows individuals to borrow money directly from other individuals or investors, bypassing traditional financial institutions like banks that operates through online platforms that connects borrowers with investors, offering unsecured personal loans, debt consolidation, or small business financing.

(c) Customer Risk

Institutions shall identify customer categories that may present higher ML/TF/PF risks such as:

- i. customers conducting transactions under unusual or suspicious circumstances;
- ii. customers with complex or opaque ownership structures that obscure beneficial ownership
- iii. foreign financial institutions;
- iv. non-bank financial institutions;
- v. Politically Exposed Persons (PEPs), their family members, and close associates;
- vi. non-resident customers and foreign account holders;
- vii. legal persons and arrangements, including shell companies and entities incorporated in higher-risk jurisdictions
- viii. cash-intensive businesses;
- ix. non-profit organisations identified by the national risk assessments as posing a higher risk of terrorism financing.
- x. trust and company service providers.

(d) Delivery Channel

Institutions shall assess risks associated with delivery channels, including:

(i) Face-to-Face Channels

- i. Risks associated with the use of false or stolen identification documents.
- ii. Movement of large volumes of cash.
- iii. Structuring or layering of transactions to evade reporting thresholds.
- xvi. Collusion between customers and staff.

ii) Non-Face-to Face Channels

- i. Challenges in verifying customer identity.
- ii. Increased potential for anonymity.
- iii. Exposure to cyber-enabled financial crime.
- iv. Use of virtual assets or digital payment methods.
- v. Circumvention of CDD measures where authentication controls are weak.

(iii) Agent and Intermediary Channels

- i. Reduced oversight of customer onboarding processes.
- ii. The risk of agent misconduct or collusion.
- iii. Ltd. visibility of beneficial ownership and control of funds.
- iv. Potential non-compliance with AML/CFT/CPF obligations.

5.2.2.3 Risk Mitigation and Controls

Institutions shall utilize the findings of the risk assessment to:

- (a) Establish and maintain policies, procedures, and controls to manage and mitigate identified ML/TF/PF risks.
- (b) Monitor the effectiveness of such policies, procedures, and controls and enhance them where necessary.
- (c) Where higher risks are identified, institutions shall implement enhanced measures to manage and mitigate those risks, where lower risks are identified apply simplified measures.
- (d) Oversight of AML/CFT policies, controls, and associated risks.

5.3 The AML/CFT/CPF Governance Framework

5.3.1 The Board of Directors – Roles and Responsibilities

The Board of Directors remains ultimately responsible for oversight of the AML/CFT/CPF program. In cases where oversight of the AML/CFT/CPF program is delegated to a designated Board committee, the Board shall ensure the committee is mandated, well- resourced, and receives regular reports to enable effective oversight of the AML/CFT/CPF function.

The Board shall:

- (a) Approve the institution's AML/CFT/CPF internal controls, policies and procedures.

- (b) Oversee an AML/CFT/CPF risk assessment, including the identification and mitigation of ML/TF/PF risks.
- (c) Monitor and assess the effectiveness of the institution's AML/CFT/CPF program. This includes ensuring prompt remediation of deficiencies, in response to evolving risks, regulatory developments and inspection findings.
- (d) Ensure that senior management effectively implements Board-approved AML/CFT/CPF policies and is held accountable for addressing deficiencies and compliance failures.
- (e) Appoint a suitably qualified and independent Money Laundering Reporting Officer (MLRO) at senior management level who shall report directly to the Board or a designated Board committee.
- (f) Ensure that the appropriate AML/CFT/CPF training is provided to Board members, senior management, and staff, commensurate with their roles and exposure to ML/TF/PF risks.
- (g) Where applicable, ensure the effective implementation of group-wide AML/CFT/CPF policies and oversight of branches and subsidiaries, including those operating in higher-risk jurisdictions.
- (h) Ensure that adequate financial, human, and technological resources are allocated to support the effective implementation of AML/CFT/CPF program.
- (i) Ensure that the AML/CFT/CPF controls are subject to regular independent testing and that identified weaknesses are remediated in a timely manner.
- (j) Ensure that the institution cooperates with the relevant competent authorities on AML/CFT/CPF matters.

5.3.2 Senior Management – Roles and Responsibilities

Senior management shall:

- (a) Be responsible for the effective implementation, day-to-day management, and ongoing operations of an institution's AML/CFT/CPF framework, in accordance with Board-approved policies and the applicable Kenyan AML/CFT/CPF laws and regulations.
- (b) Conduct and maintain institutional ML/TF/PF risk assessments.
- (c) Implement effective policies and procedures on AML/CFT/CPF measures including customer due diligence (CDD), enhanced due diligence (EDD), ongoing monitoring, sanctions screening, and suspicious transaction reporting processes and targeted financial sanctions related to terrorism financing and proliferation financing.
- (d) Submit reports to the Board or a designated committee on the institution's ML/TF/PF risks, compliance status, statistics on suspicious transaction reporting, audit findings, and regulatory or supervisory matters.

- (e) Support the MLRO, ensuring they are able to exercise sufficient authority, independence, access to information, and resources to discharge their responsibilities effectively.
- (f) Develop and implement regular training programs for the board, senior management and staff that are commensurate with their roles, responsibilities, and exposure to ML/TF/PF risks.

5.4 The AML/CFT/CPF Compliance Program

An institution shall put in place an effective AML/CFT/CPF compliance program that :

- (a) Is commensurate with an institution's size, complexity and risk profile, and addresses the ML/TF/PF risks through the institution's enterprise wise risk assessment.
- (b) Enhances the institution's ability to prevent the misuse of the financial system by identifying, assessing, monitoring, mitigating and managing associated ML/TF/PF risks.
- (c) Is documented and establishes clear roles, responsibilities and accountabilities to ensure that the appropriate policies, procedures and controls are implemented, maintained and regularly reviewed and updated.

5.4.1 Internal Controls

Institutions shall establish and maintain internal policies, procedures, systems, and controls to prevent and mitigate ML/TF/PF risks that are commensurate with the nature, scale, complexity, and ML/TF/PF risk profile of the institution.

Institutions shall, at a minimum:

- (a) Establish compliance management arrangements, including the appointment of a designated Money Laundering Reporting Officer (MLRO) at a senior management level with responsibility for overseeing compliance with AML/CFT/CPF obligations.
- (b) Implement screening procedures to ensure high standards of integrity and competence when recruiting and appointing employees.
- (c) Establish and maintain an ongoing AML/CFT/CPF training programme for directors, senior management, employees, and, where appropriate, agents, to ensure they understand their responsibilities and are able to identify and report suspicious activities.
- (d) Establish an independent audit function to periodically assess the adequacy and effectiveness of the institution's AML/CFT/CPF policies, procedures, systems, and controls, and to report its findings to senior management and the Board.
- (e) Ensure that identified deficiencies are addressed promptly and that appropriate

remedial measures are implemented.

5.4.1.1 The Money Laundering Reporting Officer (MLRO)

An institution shall:

- (a) Appoint a Money Laundering Reporting Officer (MLRO) who act as the central point of contact with CBK and the FRC for AML/CFT/CPF purposes.
- (a) Ensure that the appointment or removal of the MLRO shall be communicated to the FRC within fourteen days of their appointment or removal.
- (b) The officer shall have the necessary authority and level of seniority to carry out the function.
- (c) The institution shall provide the MLRO with the necessary resources and access to systems and records to enable to fulfil his/her responsibilities.
- (d) Ensure that the role and responsibilities of the MLRO include:
 - i. Receipt and review of suspicious transaction reports (STRs) from staff.
 - ii. Filing STRs with the FRC.
 - iii. Developing the institution's AML/CFT/CPF compliance program.
 - iv. Monitoring the AML/CFT/CPF compliance program and ensuring that it is enforced within the institution.
 - v. Coordinating training of the Board, senior management and staff on AML/CFT/CPF awareness, detection methods.
 - vi. Maintain close co-operation and liaison with the CBK and the FRC on AML/CFT/CPF related matters.

5.4.1.2 Know Your Employee Controls

Each institution shall institute specific “know your employee” controls designed to deter internal fraud and abuse of the institution which require employees to:

- (a) Follow a code of ethics.
- (b) Avoid and disclose conflicts of interest.
- (c) Maintain good credit ratings.
- (d) Adhere to policies on rotation of duties and mandatory vacations.
- (e) Require the use of employee identification cards for access to secure area.
- (f) Allocate adequate resources to effectively implement and administer the institution's AML/CFT/CPF compliance program that reflect of its size, risk profile and complexity.

5.4.1.3 The Independent Audit Function

- (a) An institution shall establish an independent audit function for the AML/CFT/CPF function.

- (b) The scope of the independent audit shall, at a minimum, assess the institution's:
 - i. Compliance with Kenya's AML/CFT/CPF laws and regulations including POCAMLA, POTA and the regulations issued thereunder and any additional guidance, directives and circulars issued by CBK and the FRC.
 - ii. Compliance with the institution's internal AML/CFT/CPF policies and procedures.
 - iii. The adequacy and effectiveness of the AML/CFT/CPF compliance programme.
 - iv. The reliability, integrity, and timeliness of internal and regulatory reporting systems, as well as management information systems.

5.4.2 Group Wide Programmes

Where an institution forms part of a financial group, it shall establish, implement and maintain a group-wide AML/CFT/CPF programme applicable to all branches and majority-owned subsidiaries.

The programme shall, at a minimum:

- (a) Establish policies, procedures and controls for the timely sharing of information required for CDD and ML/TF/PF risk management across the group.
- (b) Require the exchange of relevant customer, account and transaction information, including information on unusual or suspicious transactions or activities where appropriate, between branches, subsidiaries and group-level compliance, audit or AML/CFT/CPF functions to support AML/CFT/CPF compliance and risk management.
- (c) Establish appropriate safeguards to ensure the confidentiality, secure use and protection of information exchanged within the group, including measures to prevent tipping-off.

5.4.3 Compliance by Foreign Branches and Subsidiaries

- (a) An institution shall ensure that its foreign branches and majority-owned subsidiaries apply AML/CFT/CPF measures that are consistent with Kenya's AML/CFT/CPF laws and regulations.
- (b) In cases where Kenya's AML/CFT/CPF laws and regulations are more stringent than the host country's requirements, the foreign branches shall endeavour to comply with the Kenyan laws to the extent permitted by the host country's laws and regulations.
- (c) In cases where the host country's laws and regulations do not permit full compliance with the Kenyan AML/CFT/CPF laws and regulations the branch

or subsidiary shall immediately notify the parent institution. The institution shall notify the CBK and implement appropriate additional measures.

5.5 Customer Due Diligence

The principle of “Know Your Customer” (KYC) remains fundamental to the prevention of money laundering, terrorism financing and proliferation financing (ML/TF/PF). Effective KYC enables institutions to understand their customers, the nature and purpose of business relationships, and the expected pattern of transactions. This understanding forms the basis for applying appropriate customer due diligence (CDD) measures and implementing effective risk-based controls.

5.5.1 Customer Identification and Verification

Customer identification and verification are essential elements of the CDD process and enable institutions to establish and confirm the identity of their customers and persons acting on their behalf. The nature and extent of information required will depend on the type of customer, the nature of the business relationship, the products or services provided and the level of ML/TF/PF risk associated with the relationship.

When identifying and verifying the identity of a customer the institution is confirming that:

- (a) the customer is a real person;
- (b) the customer is who they claim to be; and
- (c) where a person the person purporting to establish or operate the relationship is the person they acts on behalf of another person, that person has been identified and verified and is duly authorised to act on behalf of the customer.

5.5.2 When Identity Must Be Verified

An institution must identify its customer in the following circumstances:

- (a) When establishing initial business relationships.
- (b) When undertaking occasional or one-off transactions.
- (c) When carrying out occasional transactions that are wire transfers.
- (d) When there is cause to be suspicious.
- (f) When there is doubt about the veracity or adequacy of previously obtained information.

5.5.3 Person Purporting to Act on Behalf of a Customer

Where a person is purporting to act on behalf of a customer, an institution shall:

- (a) Verify that the person is so authorised to act on behalf of the customer.
- (b) Identify and verify the identity of the person so authorised.

Documents that that may be used to verify that a person has been authorised to act on behalf of a customer include:

- Power of Attorney, a notarised or registered document granting the person legal authority to act on behalf of a customer.
- Board Resolution: (for customers that are legal persons) stating that the individual has been appointed to act on behalf of the entity.
- Letter of Authorisation: Signed by the customer or legal entity, specifying the scope and duration of authority.
- Partnership Agreement / LLP Deed: Specifies roles and who can act on behalf of the firm.
- Trust Deed or Trustee Resolution: If dealing with a trust, confirm the individual is a trustee or an appointed agent.

5.5.3 Prohibition on Anonymous Accounts

Institutions are prohibited from opening or maintaining anonymous accounts or accounts in fictitious names. An anonymous account is an account where the identity of the customer or beneficial owner has not been identified and verified using reliable and independent source documents, data, or information.

Examples of anonymous accounts include:

- i. Accounts opened using fictitious identities, stolen credentials, or unverified aliases.
- ii. Corporate or trust accounts where the ultimate beneficial owner (UBO), the actual natural person controlling the or operating the account is intentionally concealed.
- iii. Wallets or digital accounts on exchanges that do not require CDD to be conducted before permitting transactions.

5.5.4 Numbered Accounts

A numbered account is a bank or financial institution account that is identified primarily by a unique number, code, or other identifier instead of the customer's name in routine internal records, transaction processing, or communications. The identity of the account holder is known to the financial institution and can be accessed by authorized personnel when required for confidentiality purposes only.

Institutions that offer numbered accounts shall ensure that:

- (a) Numbered accounts are subject to CDD and, where applicable, enhanced due diligence (EDD) are conducted prior to opening the account.
- (b) The true identity and beneficial ownership of the customer are verified and documented.
- (c) The numbered accounts are subject to the full range of applicable AML/CFT/CPF preventive measures including monitoring, screening, record-keeping, and reporting obligations such as all other standard accounts.
- (d) Numbered accounts should not be used to conceal the customer's identity from competent authorities, regulators and auditors.
- (e) Transactions conducted through numbered accounts shall be monitored for suspicious activity on a risk-sensitive basis.

5.5.5 CDD Measures

Institutions shall apply the following CDD measures to all customers:

- (a) Identify and verify the customer's identity using reliable and independent source documents, data or information.
- (b) Identify the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner to ensure that the institution is satisfied that it knows who the beneficial owner is.
- (c) Obtain information on, and understand, the purpose and intended nature of the business relationship.
- (d) Conduct ongoing due diligence on the business relationship .

5.5.6 Beneficial Ownership

As part of the minimum CDD requirements, an institution shall when dealing with a customer that is a legal person or legal arrangement identify and take reasonable measures to verify the identity of the beneficial owner.

5.5.6.1 Beneficial ownership of legal persons

- (a) The identity of the natural person(s), if any, who ultimately own or control the legal person through a controlling ownership interest.
- (b) Where there is doubt as to whether the person(s) identified under paragraph (a) are the beneficial owner(s), or where no natural person exercises control through ownership interests, the identity of the natural person(s), if any, exercising control of the legal person through other means.
- (c) Where no natural person is identified under paragraph (a) or (b), the identity of

the natural person who holds the position of senior managing official.

5.5.6.2 Beneficial ownership of customers that are legal arrangements

- (a) For trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries class of beneficiaries, and any other natural person exercising ultimate effective control over the trust including through a chain of control or ownership.
- (b) For other types of legal arrangements, the identity of persons in equivalent or similar positions.

Examples of how to determine the beneficial ownership of various types of legal entities refer to **Annex II**.

5.5.7 CDD Documentation

An institution shall require every customer to provide valid, reliable and independent source documents, data or information to identify and verify the customer's identity before establishing a business relationship or carrying out a transaction for which CDD is required. The requirements for the different categories of customers are outlined below.

(a) For accounts or transactions for natural persons:

(i) At a minimum the requirements are:

- a) A birth certificate; or
- b) passport; or
- c) national identity card; or
- d) drivers licence.

(ii) Additional due diligence measures that may be used to verify the identity of the customer who is a natural person include:

- a) Current residential address verified by a referee, a utility bill i.e. electricity or water bill, etc. if applicable where appropriate.
- b) Utility bill that is registered in the name of the customer.
- c) Mobile telephone number.
- d) Occupation or employment details.
- e) Source of income.
- f) Nature and location of business activity.
- g) Income tax personal identification number (PIN) issued by Kenya Revenue Authority (KRA) to the customer;

- h) Where applicable, written confirmation from customer's prior bank attesting to customer's identity and history of account relationship (bank referee).

(b) For minors' accounts

(i) at a minimum , the requirements are as follows:

- a) Nationality and date of birth evidenced by birth certificate of the minor.
- b) National passport, driving license or national identity document and certified copy of the legal parent or guardian.

(ii) Additional measures that may be used to verify the identity of a minor include:

- a) Verified address of current residence of minor and also of legal parent or guardian. The verification should be done by a referee or via the production of utility bills i.e. electricity and water bills in the name of the parents.
- b) Declaration of source of funds or income from the parent/guardian.

(c) For accounts or transactions for legal persons

(i) At a minimum the requirements are as follows:

- a) The registered name of the legal person or legal entity.
- b) Evidence of registration or incorporation, including a certified copy of the Certificate of Registration, Certificate of Incorporation, Memorandum and Articles of Association, Partnership Deed, or other similar documentation evidencing the legal status of the legal person or legal entity.
- c) The address of the registered office and, where different, the principal place of business.
- d) A certified copy of a board resolution authorising the opening of an account, conducting business with the institution and where applicable, borrowing funds, and identifying the persons authorised to act as signatories on behalf of the legal person or legal entity.
- e) The full name, date of birth, identification or passport number, and address of natural persons who manage, control or own the legal person or legal entity.

- f) Audited financial statements for the most recent full financial year, where the customer is a corporate body.
- g) Unaudited financial statements for the most recent full financial year, where the customer is a sole trader. An institution may consider exempting a newly established sole proprietorship or corporate body that has been in existence for less than one year, where there are practical difficulties in obtaining financial statements;
- h) The customer's personal identification number, where applicable.
- i) Written confirmation from the customer's previous bank, where applicable, confirming the customer's identity and account relationship history.

(d) For accounts or transactions for partnerships

- a) The name of the partnership or where applicable its registered name.
- b) The Partnership Deed.
- c) The registered address or principal place of business or office of the partnership.
- d) The registration number the full name, date of birth, identity card number or passport number and address of every partner.
- e) The person who exercises executive control over the partnership.
- f) The name and particulars of each natural person who purports to be authorised to establish a business relationship or to enter into a transaction with the institution on behalf of the partnership. Un-audited financial statements for the last full year: Provided that an exemption may be considered by an institution for a new partnership which has not been in existence for more than a year in the production of un-audited financial statements.

(e) For accounts or transactions for legal arrangements such as trusts:

(i) At a minimum the requirements are as follows:

- (a) Registered name of the trust.
- (b) Registration number.
- (c) Evidence of registration or incorporation such as a Certificate of Incorporation or registration.
- (d) A trust deed.
- (e) A formative document such as partnership agreement, memorandum and articles of association.

- (f) Official returns showing registered office and if different the principal place of business.
- (g) Full name and details of the management company of the trust or legal arrangement, if any.
- (h) Names of the relevant persons having senior management position in the legal person or trustees of the legal arrangement.
- (i) Full names of the trustee, beneficiaries or any other natural person exercising ultimate effective control over the trust
- (j) Full names of the founder of the trust.
- (k) Any other documentation from a reliable independent source proving the name, form and current existence of the customer.

(f) For accounts or transactions for un-incorporated businesses/partnerships

- a) Where the applicant is an un-incorporated business or a partnership whose partners/controllers are not known to the institution, the identity of at least two partners/controllers and/or signatories to the mandate should be verified initially, in line with the requirements for personal customers. When signatories to the mandate change, care should be taken to ensure that the identity of at least two of the current signatories has been verified. For established businesses, a copy of the latest financial report and accounts (audited where applicable) should be obtained.
- b) Conduct a site visit to the place of business to confirm the true nature of the business activities. The nature of the partnership or business should be ascertained to ensure that it has a legitimate purpose. In cases where a formal partnership arrangement exists, a mandate from the partnership.
- c) Authorising the opening of an account and conferring authority on those who will operate it should be obtained.

(g) Trustees of Occupational Pension Schemes

For the Trustees of Occupational Pension Schemes, satisfactory verification of identity can be based on the inspection of formal documents concerning the Trust which confirm the names of the current Trustees and their addresses for correspondence. Verification can also be based on extracts from Public Registers, or references from Professional Advisors or Investment Managers.

(h) For Non-Kenyan Residents

Institutions shall:

- (a) Identify and verify the customer using reliable and independent source documents, data or information, including a valid passport or other official

- identification document issued by the relevant competent authority.
- (b) (Verify the customer's residential and contact information, including the customer's address in the country of residence, using reliable and independent sources.
 - (c) Where applicable, establish the customer's status in Kenya, including obtaining appropriate evidence of immigration status where the customer is resident in Kenya, such as a foreign certificate (alien card), work permit or passport bearing an entry stamp.
 - (d) Establish the purpose and intended nature of the business relationship, including the reasons for maintaining an account or obtaining financial services in Kenya and, where relevant, the expected nature and volume of cross-border transactions.
 - (e) Identify and verify any person acting on behalf of the customer and establish that person's authority to act.
 - (f) Where the customer is a legal person or legal arrangement, identify and verify the beneficial owner(s) and understand the ownership and control structure.
 - (g) Obtain information on the source of funds and, where appropriate based on the risk, the source of wealth.
 - (h) Identify the beneficial owner(s) and persons acting on behalf of the customer for applicable PEP, sanctions and other relevant ML/TF/PF risks.
 - (i) Assess the risks associated with the customer's country of residence, nationality, business activities and expected transaction flows, including exposure to jurisdictions presenting higher ML/TF/PF risks.
 - (j) Apply enhanced CDD and ongoing monitoring where higher ML/TF/PF risks are identified, in accordance with applicable law and the institution's risk-based approach.

5.5.8 National Government or Quasi-Government and County Government Institutions Subject to Prior Authorisation or Other Preconditions

Where the establishment or operation of an account or transaction for a customer that is a national government quasi- government institution that is subject to prior authorisation, licensing, registration or other preconditions under the applicable legal or regulatory framework, institutions shall, in addition to complying with the CDD requirements prescribed under POCAMLA and the POCAML Regulations:

Examples of these types of organisations and institutions and the relevant authorisation and preconditions that apply are highlighted below:

i. Ministries /State Departments

For accounts opened for a national government ministry or State Department, the

bank should obtain:

- (a) Formal written authority from the National Treasury to the responsible Accounting Officer authorizing the opening and operation of the account, with evidence that the authority has been copied to the Controller of Budget and the Auditor-General.
- (b) Where the account is to be maintained with a commercial bank, documentary evidence of the applicable approval or exception under Regulation 82, including Cabinet Secretary approval where required.
- (c) Formal account-opening request or instruction from the Accounting Officer stating the purpose of the account and, where applicable, the funding source.
- (d) Appointment/designation documents for the Accounting Officer and authorized signatories, together with the approved account mandate, signing instructions and specimen signatures.
- (e) Identification and CDD documents for authorized signatories, including staff IDs, national IDs/passports, KRA PINs and official contacts.
- (f) Applicable National Treasury banking rules or operating conditions, including transaction limits or maximum balance, and confirmation that the account shall not be overdrawn or used to obtain an unauthorized advance or loan.

ii. State Corporations /Parastatals

For accounts opened by a State corporation/parastatal, the bank should obtain:

- (a) Legal instrument establishing the entity, such as the enabling Act, Legal Notice, Gazette Notice, certificate of incorporation or other constitutive instrument.
- (b) Certified Board/governing-body resolution or equivalent internal approval authorizing the opening of the account, its purpose, the proposed signatories and the banking mandate, where applicable.
- (c) Written National Treasury authority where the entity and account are subject to section 28 of the Public Finance Management(PFM) Act and Regulation 82 of the National Government Regulations.
- (d) Where a commercial-bank account is proposed under the PFM framework, documentary evidence of the applicable Regulation 82 exception or Cabinet Secretary approval for special circumstances.
- (e) Evidence of the appointment or authority of the Accounting Officer, Chief Executive Officer or other officer authorized to act for the entity, together with the account mandate and specimen signatures.
- (f) Identification and CDD documents for authorized signatories, including national IDs/passports, KRA PINs and official contacts
- (g) Information on the account purpose and source of funds sufficient to establish the applicable PFM banking treatment, including whether the entity draws

more than 75 percent of its resources from the National Exchequer Account.

iii. NG/CDF Project Account

- (a) Resolution of the Constituency Committee authorising the opening of the project bank account;
- (b) A Resolution of the Project Management Committee, recorded in the minutes of the Committee, appointing the signatories to the bank account; and
- (c) An official introduction of the Project Management Committee and its appointed signatories to the bank by an Officer of the Board
- (d) A change of signatories upon receipt and verification of the required authorisation and supporting documentation.

Constituency Committee Responsibility

For avoidance of doubt, the Constituency Fund account and a Project Management Committee project account are separate accounts and shall be subject to their respective approval and operational requirements.

iv. County Government Treasury / County Bank Account

For accounts opened in the name of a county government, county treasury, county revenue fund, county exchequer account, or county treasury single account/sub-account, a bank should obtain:

- (a) Formal written authority from the County Treasury signed by the Chief Officer responsible for finance.
- (b) Evidence that the authority has been copied or notified to the Controller of Budget and the Auditor-General .
- (c) County Treasury banking rules, including account purpose, authorized transactions, signatory mandate, operating limits, and the maximum balance permitted for the account.
- (d) Specimen signatures and identification documents for authorized signatories, including appointment letters, staff IDs, national IDs/passports, KRA PINs, and official contacts.
- (e) Resolution, instruction, or internal approval showing the purpose of the account, for example revenue collection, imprest, project implementation, conditional grant, health facility operations, or municipal services.
- (f) Mandate requires bank statements or account information to be made available to the County Treasury/CECM for Finance.
- (g) Confirmation that the account shall not be overdrawn and that no advance or loan shall be obtained through the account unless authorized under the PFM framework.

v. Other County Government Entities

Examples include health facilities, municipal boards, county public funds, county corporations, county agencies.

For accounts opened by a county government entity, the bank should obtain:

- a) Formal written authority from the County Treasury, signed by the Chief Officer Finance.
- b) Evidence that the authority has been copied to the Controller of Budget and Auditor-General.
- c) Extract of Board, committee, or management minutes/resolution approving the opening of the account, identifying the purpose of the account, approving proposed signatories, and authorizing the banking mandate.
- d) Appointment letters or gazette notices for the signatories and accounting officer, confirming their authority to act for the entity.
- e) Legal instrument establishing the entity, such as:
 - County legislation
 - Gazette notice
 - municipal board appointment notice;
 - county corporation incorporation/statutory instrument;
- f) Account operating instructions, including signing rules, approval thresholds, transaction limits, permitted credits/debits, and maximum balance prescribed by County Treasury.

vi. Donor-Supported / Grant-Funded County Accounts

For donor-supported county accounts, the bank should obtain:

- (a) Grant, donation, financing, or project agreement between the county government/county entity and the donor/development partner.
- (b) Approval by the County Executive Committee Member for Finance to receive the grant/donation.
- (c) County Treasury authority to open and operate the project account, copied to the Controller of Budget and Auditor-General.
- (d) Confirmation of whether funds are to be paid into the County Revenue Fund first, then released to the project account.

5.6 Ongoing Due Diligence

An institution shall conduct ongoing due diligence on the business relationship by:

- (a) scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the reporting institution's knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and
- (b) Ensuring that documents, data or information collected under the CDD process is kept up-to date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.

5.7 Enhanced Customer Due Diligence Measures

Enhanced due diligence (EDD) measures shall be applied to persons and entities that present a higher risk to the institution. This can broadly be addressed through the following measures:

- (a) Obtain additional information to establish the customer's identity.
- (b) Apply additional measures to check documents supplied by a financial institution.
- (c) Obtain senior management approval for the new business relationship or transaction.
- (d) Establish the customer's source of wealth.
- (e) Conduct ongoing monitoring of the business relationship.

5.8 Simplified Due Diligence Measures

- (a) An institution may apply simplified due diligence (SDD) measures where a customer or business relationship has been assessed as presenting a lower ML/TF/PF risks, based on the institution's risk assessment and taking into account the findings of the national risk assessment, where applicable.
- (b) Where simplified measures are applied, they must be proportionate to the level of identified risk.
- (c) An institution shall not apply SDD measures in the following circumstances:
 - (i) Where there is knowledge, suspicion or reasonable grounds to suspect money laundering, terrorist financing or proliferation financing.
 - (ii) Where a higher-risk scenario has been identified, such as:
 - (iii) Where the customer or beneficial owner is a Politically Exposed Person (PEP).
 - (iv) Where the customer or transaction has links to a high-risk jurisdiction or country subject to sanctions.
 - (v) Where the ownership or control structure of a customer that is a legal person or legal arrangement is unusually complex or lacks transparency.

- (vi) Where transactions are unusual, complex or inconsistent with a customer's known profile.
- (vii) Where the institution is unable to satisfactorily verify the customer's identity, beneficial ownership or source of funds, where applicable.

5.9 Non-Face-To-Face Verification

5.9.1 General Requirements

Institutions shall:

- (a) Establish and maintain policies, procedures and controls on non-face-to face verification of customers.
- (b) Apply non-face to face verification measures that are proportionate to the ML/TF/PF risks presented by the customer.

5.9.2 Non-Face to - Face - Identification and Verification of Natural Persons

- (a) Institutions shall determine the appropriate verification measures to be undertaken using reliable documentation, electronic, biometric or other appropriate measures, including:
 - (i) government-issued identification documents or other official means of identification prescribed under POCAMLA and the POCAML Regulations;
 - (ii) electronic verification of identification documents, including checks of their authenticity, validity and integrity; and
 - (iii) verification against reliable and independent government or other authoritative databases, where the institution is authorised to access and use such information, such as the Integrated Population Registration System (IPRS) or the Kenya Revenue Authority (KRA) portal.
- (b) Where a prospective non-Kenyan resident customer is unable to be physically present for identification and verification, an institution may apply alternative reliable and independent verification measures, including:
 - (i) confirmation of the customer's identity and address details through a branch, subsidiary, head office, representative office or correspondent bank in the prospective customer's country of residence;
 - (ii) obtaining a copy of the customer's passport authenticated by the embassy of the customer's home country in Kenya; or
 - (iii) obtaining an account-opening reference from a reputable financial institution in the applicant's home country, including verification of the

customer's true name or names used, current permanent address, date of birth and signature.

5.9.3 Verification of Address and Contact Information

Where verification of a customer's physical, residential, postal or business address is required, an institution shall take reasonable measures to establish the accuracy of the information provided using reliable and independent sources taking into account the customer's circumstances and risk profile.

Depending on the circumstances, the verification of address information may be verified using documentary, electronic or other reliable sources, including:

- (a) government-issued documents or official records containing address information;
- (b) reliable electronic or digital databases, where the institution is authorised to access and use such information;
- (c) bank or other financial institution statements;
- (d) tenancy or lease agreements;
- (e) property ownership or other relevant property records;
- (f) official correspondence issued by a government or public authority;
- (g) utility or other service records;
- (h) independently verifiable electronic or digital information;
- (i) confirmation from a landlord, property manager or other appropriate third party, where supported by reliable information; or
- (j) other reliable and independent sources capable of reasonably establishing the customer's address.

5.9.4 Verification of Legal Persons and Legal Arrangements

Where a legal person or legal arrangement is established through a non-face-to-face channel, the institution shall apply appropriate measures to verify:

- (a) the legal existence and registration status of the legal person or legal arrangement using foundational documents such as Certificate of Registration and Memorandum of Articles of Association;
- (b) the identity of persons authorised to act on behalf of the customer;
- (c) the identity of directors, partners, trustees or other relevant persons, as applicable;
- (d) the beneficial owners and persons exercising ultimate effective control;
- (e) the purpose and intended nature of the business relationship; and
- (f) the nature of the customer's business or activities and the expected transaction profile. Verification may include the use of the Business Registration Service (BRS), reliable databases, official electronic records, information provided by the customer and other reliable and independent sources.

5.9.5 Non-Face – to - Face Identification and Verification of the Customer - Through Digital Channels

For purposes of this section, digital banking means the provision of banking products or services through electronic or digital channels that enables a customer to establish, access or operate a banking relationship without being physically present at the institution. This includes internet banking, mobile banking applications, digital platforms, digital account opening and onboarding, and other electronic or technology enabled channels through which customer identification and verification are undertaken.

- (a) Where an institution conducts customer identification and verification through digital banking channels, it shall comply with the requirements of this Guideline and the relevant sections of the POCAMLA and POCAML Regulations on CDD and shall apply appropriate measures to establish and verify the identity of the customer commensurate with the ML/TF/PF risks associated with the digital channel.
- (b) Where appropriate, institutions may use electronic or digital means to identify and verify customers, including:
 - (i) electronic verification of identity documents;
 - (ii) digital identity or electronic identification systems;
 - (iii) biometric verification, including facial or fingerprint recognition;
 - (iv) liveness detection or equivalent measures designed to establish that the individual presenting for verification is physically present and is not using a photograph, recording, manipulated image or other artificial means to impersonate another person;
 - (v) video identification or other appropriate remote visual verification; and
 - (vi) other reliable technological means capable of providing an appropriate level of assurance regarding the identity of the customer.
- (c) Institutions shall ensure that digital identification and verification measures are sufficiently robust to mitigate the risks of identity-related fraud including but not limited to:
 - (i) Impersonation, the fraudulent representation by a person that they are another individual or entity, usually to deceive, obtain access, or facilitate an unlawful transaction.
 - (ii) Identity theft, which is the unauthorised acquisition, use or misuse of another person's personal or identifying information for fraudulent or unlawful purposes.
 - (iii) SIM Swap where an unauthorised person induces or causes a mobile network operator or service provider to transfer a subscriber's mobile

service credentials from the subscriber's legitimate Subscriber Identity Module (SIM) to a SIM under the unauthorised person's control, thereby transferring control of the associated mobile number and enabling access to voice, SMS, data, or other services linked to that number.

- (iv) Synthetic identities where fictitious identities are created by combining genuine personal information with fabricated information to establish a false identity for fraudulent or other unlawful purposes.
- (v) Spoofing where the deliberate falsification or manipulation of identifying information, digital communications to deceive a person, system or institution as to the true identity, source or destination of a communication or transactions.

5.9.7 CDD and Data Protection

Where digital or electronic means are used for customer identification and verification, institutions shall:

- (a) Process customer data in accordance with applicable data protection requirements, under the Data Protection Act and applicable regulations. Particular care shall be taken where the process involves biometric or other sensitive personal data, photographs, video recordings, identity documents, device or location information.
- (b) Ensure that customer data collected is relevant and Ltd. to what is necessary for CDD purposes, adequately protected against unauthorised access, loss, alteration, disclosure or misuse, and retained in accordance with applicable legal and regulatory requirements under the POCAMLA and POCAMLA Regulations.
- (c) Where an institution has engaged third parties to provide digital identification or verification services, ensure that appropriate arrangements are in place for the lawful processing, protection, storage and retention of customer data and, where applicable, comply with requirements relating to data protection under the Data Protection Act.

5.10 Reliance on Third Parties

These requirements do not apply to outsourcing or agency arrangements where the service provider or agent is treated as part of the institution.

For the purposes of this section, a third party means a financial institution or designated non-financial business or profession (DNFBP) that is regulated, supervised or monitored for compliance with AML/CFT/CPF requirements and on which an institution may rely to perform specified CDD measures.

- (a) An institution may rely on a third party to perform elements of CDD¹ or to introduce business, provided that where it is relying on a third party:
 - (i) Bears the ultimate responsibility for compliance with the CDD measures.
 - (ii) Shall immediately obtain the necessary information relating to the key elements of CDD concerning the relevant elements of CDD measures as required.
 - (iii) Take steps to establish that copies of identification data and other relevant documentation relating to the CDD measures will be made available by the third party without delay upon request; and ascertain that the third party:
 - i. Is regulated, supervised or monitored for compliance with AML/CFT/CPF requirements by a competent authority.
 - ii. Has put in place measures to comply with the CDD and record-keeping requirements set out in Kenya's AML/CFT/CPF legislation including these Guidelines.
- (b) Where an institution relies on a third party established in another jurisdiction, it shall take into account the level of country risk when determining whether reliance on that third party is appropriate.
- (c) Where an institution relies on a third party that forms part of the same financial group, the requirements of paragraphs (a) to (d) above may be regarded as satisfied where:
- (d)
 - (i) the financial group applies CDD, record-keeping and politically exposed person (PEP) requirements, together with group-wide AML/CFT/CPF programmes, consistent with these Guidelines;
 - (ii) the implementation of those CDD, record-keeping and AML/CFT/CPF programmes is subject to effective group-level oversight by a competent authority; and
 - (iii) any higher country risk is adequately mitigated through the group's AML/CFT/CPF policies, procedures and controls.

5.11 Failure to complete CDD Measures

Where an institution is unable to fully comply with CDD requirements:

- (a) Prior to opening an account, it shall not open the account, commence the business relationship or perform or undertake the transaction and submit a suspicious transaction report (STR) to the FRC.

¹ identification and verification of the customer /beneficial owner; and obtaining information on the purpose and intended nature of the business relationship or transaction.

- (b) In cases where it has already commenced the business relationship with the customer, it shall terminate the business relationship and file an STR with the FRC.

5.12 Politically Exposed Persons (PEPs)

For purposes of this section, a Politically Exposed Person(PEP) means:

- (a) A Foreign PEP, A person who has been entrusted with a prominent public in another jurisdiction including:
 - (i) Heads of State or Government;
 - (ii) members of Cabinet;
 - (iii) State Officers;
 - (iv) Senior Public Officers;
 - (v) Senior executives of state-owned corporations;
 - (vi) Senior military officials and other senior members of the disciplined forces;
 - (vii) A Domestic PEP, a person who has members of the Judiciary;
- (b) been entrusted with a prominent public in Kenya holding the positions highlighted in 5.12 a) (i)-vii) above.
- (c) Persons who are or have been entrusted with a prominent function by an international organisation to senior management positions, i.e. directors, deputy directors and members of the board or equivalent functions.
- (d) Any immediate family member or close business associate of persons referred to from 5.12 (a) to (c).

5.12.2 CDD Measures for Categories of PEPs

5.12.2.1 Foreign PEPs

In the case of foreign PEPs, in addition to performing the CDD an institution shall:

- (a) Put in place risk management systems to determine whether a customer or the beneficial owner is a PEP;
- (b) Obtain approval from senior management to transact/establish the relationship with that person.
- (c) Take adequate measures to establish the source of wealth and the source of funds which are involved in the proposed business relationship of transaction.
- (d) Once the account has been established, conduct enhanced on-going monitoring of the relationship.

5.12.2.2 Domestic PEPs and Persons Entrusted with a Prominent Function by an International Organisation

In relation to Domestic PEPs or persons who have been entrusted with a prominent function by an international organisation, in addition to performing the CDD measures required under 5.6.5 of this Guideline, institutions shall:

- (a) Take reasonable measures to determine whether a customer or the beneficial owner is a PEP; and
- (b) In cases when there is higher risk business relationship with such a person, apply the measures highlighted under 5.12.2.1 (b-d).

5.12.2.3 Immediate Family Members or close Business Associates

Institutions shall apply the measures outlined in 5.12.2.1 (a-d) and 5.12.2.2 (a-b) for family members or close associates of all types of PEP where applicable.

5.12.3 PEPs - Life Insurance Policies Payout

- (a) An institution shall implement risk based measures to determine whether a beneficiary of a life insurance policy and, where applicable, the beneficial owner of the beneficiary, is a PEP. Such measures shall be undertaken no later than the time of the policy payout.
- (b) Where a beneficiary or the beneficial owner of the beneficiary is identified as a PEP, or where the relationship presents a higher risk of money laundering, terrorist financing, or proliferation financing, the institution shall:
 - (i) Inform and obtain approval from senior management prior to the payment of policy proceeds;
 - (ii) Conduct enhanced due diligence (EDD) and enhanced scrutiny of the entire business relationship, including the source of funds and the legitimacy of the policy benefits;
 - (iii) Assess whether the payment or the business relationship gives rise to suspicion of money laundering, terrorist financing, proliferation financing, or any other financial crime;
 - (iv) Consider whether an STR should be submitted to the FRC;
 - (v) Document the risk assessment, the enhanced due diligence measures applied and the rationale for the decision to proceed with or delay the payout, and all approvals obtained.
 - (vi) In the event that that a customer subsequently becomes a PEP after having initially established a relationship with a financial institution, the institution is to carry out steps a) to c) above immediately it is made aware that a customer is a PEP.

5.13 Correspondent Banking

An institution which intends to establish a correspondent banking relationship either as the correspondent bank or the respondent bank shall undertake the following steps before establishing a business relationship:

- (a) Gather sufficient information about the correspondent bank regarding the nature of its business activities.
- (b) Determine from available information the reputation of the correspondent bank institution and the quality of its supervision.
- (c) Determine the quality of AML/CFT/CPF laws and regulations in the correspondent bank's jurisdiction or country of domicile.
- (d) Assess the correspondent bank's AML/CFT/CPF controls.
- (e) Obtain approval from senior management before establishing a new correspondent banking relationship.
- (f) In respect to the correspondent bank's customers, be assured that it verifies the identity of its customers and conducts on-going monitoring.
- (g) Verify the ownership and management structures of the correspondent bank including whether a PEP has ownership or control of the bank.

5.13.1 Payable Through Accounts

With respect to payable-through accounts, an institution shall satisfy itself that the respondent financial institution has:

- (a) performed CDD obligations on its customers that have direct access to the accounts of the correspondent financial institution; and
- (b) is able to provide relevant CDD information upon request to the correspondent financial institution.

5.14 Prohibition on Shell Banks

- (a) Institutions are prohibited from opening an account or entering into a correspondent banking relationship with a shell bank.
- (b) Prior to entering into a correspondent banking relationship with another bank, an institution should ensure that the bank does not permit their accounts to be used by shell banks.

5.15 Higher Risk Countries

- (a) An institution shall apply enhanced due diligence (EDD) on business relationships and transactions with any natural and legal persons, legal arrangements, or financial institutions originating from countries identified as

posing a higher ML/TF/PF risk by:

- (b)
 - (i) The FATF as having strategic ML/TF/ deficiencies, and that have not made sufficient progress in addressing those deficiencies or have not committed to an action plan to address them; or
 - (ii) The Cabinet Secretary, National Treasury as having ongoing substantial ML/TF/PF risks.
- (c) In order to protect the financial system from ongoing and substantial ML/TF/PF risks emanating from the jurisdictions referred to under 5.15(b) (i-ii) institutions shall apply countermeasures including:
 - (i) Limiting or terminating business relationships or financial transactions with natural persons, legal persons, legal arrangements, or financial institutions located in the concerned countries.
 - (ii) Prohibiting reliance on third parties located in the concerned countries to conduct CDD.
 - (iii) Applying enhanced due diligence measures on correspondent banking relationships with financial institutions located in the concerned countries and when considering the establishment of subsidiaries, branches, or representative offices of financial institutions from the concerned countries, taking into account whether the financial institution is based in countries identified as having ML/TF/PF risks or inadequate AML/CFT/CPF framework.

5.16 Wire Transfers

5.16.1 Definitions

For purposes of this Section:

“beneficiary” means a person or legal arrangement identified by the originator as the receiver of the requested wire transfer;

“beneficiary financial institution” means a financial institution which receives the wire transfer from the ordering financial institution directly or through an intermediary financial institution and makes the funds available to the beneficiary;

“cross-border wire transfer” includes any wire transfer where either the ordering financial institution or the beneficiary financial institution is located outside Kenya and any chain of wire transfer in which at least one of the financial institutions involved is located outside Kenya;

“domestic wire transfer” includes any wire transfer where the ordering financial institution and beneficiary financial institution are located in Kenya, and any chain of wire transfer that takes place entirely within the country, even though the system used to transfer the payment message may be located in another country;

“intermediary financial institution” means a financial institution in a serial or cover payment chain that receives and transmits a wire transfer on behalf of the ordering financial institution and the beneficiary financial institution, or another intermediary financial institution;

“ordering financial institution” means a financial institution which initiates the wire transfer and transfers the funds upon receiving the request for an wire transfer on behalf of the originator; **“originator”** means an account holder who allows the wire transfer from that account, or where there is no account, the person that places the order with the ordering financial institution to perform the wire transfer.

5.16.2 Requirements for Ordering Financial Institutions

- (a) Ordering financial institutions shall ensure that all cross-border wire transfers, regardless of the amount or value of the transaction, are accompanied by complete, accurate and sufficient information to identify and trace the originator, beneficiary and transaction, including the following:
 - (i) Required and accurate originator information:
 - i. the name of the originator;
 - ii. the originator’s account number where an account is used to process the transaction or, in the absence of an account, a unique transaction reference number that permits traceability of the transaction; and
 - iii. the originator’s address, national identity number, customer identification number, or date and place of birth.
 - (ii) Required beneficiary information:
 - i. the name of the beneficiary; and
 - ii. the beneficiary’s account number where an account is used to process the transaction or, in the absence of an account, a unique transaction reference number that enables the transaction to be traced.

- (b) Where several individual cross-border wire transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the ordering financial institution shall:
 - (i) ensure that the batch file contains complete and accurate originator information and full beneficiary information for each individual transfer; and
 - (ii) each transfer remains fully traceable to the originator and beneficiary throughout the payment chain, including within the beneficiary country.
- (c) For all domestic wire transfers, an ordering financial institution shall ensure that the information accompanying the transfer includes complete and accurate originator information as specified for cross-border wire transfers, unless such information can be made available to the beneficiary financial institution and appropriate authorities by other means.
- (d) Where the information accompanying a domestic wire transfer can be made available to the beneficiary financial institution and appropriate competent authorities by other means, an ordering financial institution shall:
 - (i) include at least the account number or a unique transaction reference number or identifier, provided that the number or identifier permits the transaction to be traced back to the originator and beneficiary;
 - (ii) make the required originator and beneficiary information available within three business days of receiving a request from the beneficiary financial institution or an appropriate competent authority; and
 - (iii) make the required information available immediately upon request where the request is made by a law enforcement agency.
- (e) Ensure that all originator and beneficiary information collected in relation to wire transfers in accordance with requirements on record keeping under the POCAMLA and POCAML Regulations. This includes retaining all such records for a minimum of seven years.
- (f) An ordering financial institution shall not execute a wire transfer where the required originator or beneficiary information is not available or does not meet the requirements applicable to the transfer.

5.16.3 Requirements for Intermediary Financial Institutions

For cross-border wire transfers, intermediary financial institutions shall:

- (a) Ensure that all originator and beneficiary information accompanying a wire transfer remains with the transfer throughout the payment chain;
- (b) Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, maintain a record of all information received from the ordering financial institution or another intermediary financial

- institution for a minimum of seven years.
- (c) Take reasonable measures, consistent with straight-through processing, to identify cross-border wire transfers that lack required originator or beneficiary information;
- (d) Establish and implement risk-based policies and procedures for determining:
 - (i) When to execute, reject or suspend a wire transfer that lacks required originator or beneficiary information.
 - (ii) The appropriate follow-up action to be taken in respect of such a wire transfer.

5.16.3 Requirements for Beneficiary Financial Institutions

For cross-border wire transfers, beneficiary financial institutions shall:

- (a) Take reasonable measures, which may include post-event monitoring or real-time monitoring where feasible, to identify cross-border wire transfers that lack required originator or beneficiary information.
- (b) For all cross-border wire transfers, regardless of the amount or value of the transaction, verify the identity of the beneficiary. Where the identity has not been previously verified, maintain the identification documentation for a minimum of seven years in accordance with the requirements on record keeping stipulated in Kenya's AML/CFT/CPF laws and regulations.
- (c) Establish and implement risk-based policies and procedures for determining::
 - (i) when to execute, reject or suspend a wire transfer that lacks required originator or beneficiary information; and
 - (ii) the appropriate follow-up action to be taken in respect of such a wire transfer.

5.16.4 Implementation of Targeted Financial Sanctions

Institutions shall, in the context of processing wire transfers;

- (a) Take the necessary measures to freeze without delay funds and other assets owned or controlled, directly or indirectly, by persons or entities designated pursuant to the relevant UNSCRs concerning the prevention and suppression of terrorism and terrorist financing, including UNSCRs 1267 and 1373.
- (b) Refrain from making funds or other assets available, directly or indirectly, to or for the benefit of any designated person or entity, where such conduct is prohibited under the applicable targeted financial sanctions regime.

- c) Put in place effective policies, procedures and controls in place to identify designated persons and entities, prevent prohibited transactions, and ensure the timely implementation of freezing and prohibition measures in accordance with the POTA and the regulations issued thereunder..

5.17 Money Value or Transfer Services

Institutions that offer money value or transfer services as a product should ensure that the providers of (MVTs) are:

- a) Licensed or registered by CBK.
- b) Subject to effective systems for monitoring and ensuring compliance with AML/CFT/CP measures.
- c) Have AML/CFT programmes in place.
- d) Regularly monitor the AML/CFT/CPF programs for compliance.
- e) Maintain a current list of its agents.
- f) Ensure that the agents have been incorporated in its AML/CFT/CPF compliance programs.
- g) Ensure that the agents are subject to monitoring for AML/CFT/CPF purposes.

5.18 New Technologies

An institution shall:

- (a) Conduct a risk assessment prior to introducing a new product, business practice, delivery mechanism or new or developing technology, including technology applied to existing products, to identify and assess associated ML/TF/PF risks.
- (b) Adopt reasonable and proportionate measures to prevent the misuse of new technologies for ML/TF/PF purposes.
- (c) Implement appropriate measures to manage and mitigate identified ML/TF/PF risks.
- (d) Document the findings of the risk assessments and make them available to the FRC or other competent authorities upon request.

5.19 Reporting of Suspicious Transactions

Institutions shall:

- (a) Report suspicious activities or transactions to the FRC within forty-eight (48) hours after the suspicion arises, where the institution knows or ought reasonably to have known that the activity or transaction may involve money laundering, terrorism financing or proliferation financing;
- (b) Provide sufficient information in the report to explain the nature and basis of

- the suspicion and, where available, submit relevant supporting documentation;
- (c) Submit the STRs in line with the reporting procedures and prescribed format issued by the FRC for the submission of suspicious transaction or activity reports.
 - (d) Maintain appropriate internal procedures and controls to ensure the timely identification, escalation and reporting of suspicious activities and transactions in accordance with the applicable legal and regulatory requirements under Kenya's AML/CFT/CPF legislation.

For examples of triggers of suspicious transactions refer to **Annex III**.

5.20 Tipping Off

- (a) Institutions which obtain or become aware of information which is suspicious or indicates possible money laundering, terrorism financing or proliferation financing shall not disclose such information to the customer but report it to the FRC.

5.21 Cash Transaction Reports

Institutions shall:

- (a) File a cash transaction report (CTR) for any transaction that is equivalent to or that exceeds USD 15,000, or its equivalent in any other currency, to the FRC. This is irrespective of whether the transaction is considered suspicious.
- (b) Submit the report electronically to the FRC.
- (c) Submit the report within the prescribed timeframe, being by Friday of the week in which the transaction occurred, or any other period as may be specified by the FRC.
- (d) In instances where an institution is unable, for an acceptable reason, to submit the report electronically, use an alternative reporting method approved or accepted by the FRC such as:
 - i. Forwarding the CTR by facsimile to the Director-General at a facsimile number specified by the FRC for this purpose.
 - ii. Delivering the CTR to the offices of the FRC or to an address specified by the FRC
- (e) Submit the report without delay where the circumstances warrant immediate reporting.
- (f) Ensure that the submission of a cash transaction report, or any information relating to such report, is not disclosed to the customer or any unauthorised person where such disclosure would amount to tipping-off the customer.

Additional guidance on role of financial institutions in cash transaction reporting, monitoring is set out under **Annex IV**.

5.20 Record Keeping

Institutions shall retain records of, both domestic and international transactions for a minimum period of seven years from the date the relevant business or transaction was completed or following the termination of an account or business relationship:

- (a) Records of documentation obtained for CDD purposes including identification documents such as passports, identification cards or similar documents;
- (b) Account files ;
- (c) Business correspondence;
- (d) The results of any analysis undertaken such as inquiries to establish the background and purpose of complex, unusual, large transactions.
- (e) Any actions taken with regards to STRs filed related to targeted financial sanctions (TFS).
- (f) Where the transaction involves a negotiable instrument other than currency, the name of the drawer of the instrument, the name of the institution on which it was drawn, the name of the payee.

5.21 The Cross Border Conveyance of Monetary Instruments

Under the POCAMLA and the POCAMLA Regulations persons conveying monetary instruments into or out of Kenya equivalent to or exceeding USD 10,000, or its equivalent in Kenya shillings or any other currency, are required to declare the instruments to a customs officer at the relevant port of entry or exit in the prescribed manner. Customs officers are responsible for receiving and processing such declarations and may exercise the applicable powers of search, seizure and other enforcement measures where there are reasonable grounds to suspect a false or non-declaration.

Financial institutions also play an important role in mitigating the ML/TF/PF risks associated with the cross-border movement of monetary instruments. Institutions should consider relevant declarations, cash movements and associated customer activity when undertaking CDD, transaction monitoring and risk assessment, and should report suspicious activity to the FRC where appropriate.

PART VI: TARGETED FINANCIAL SANCTIONS

6.1 Definitions

For the purposes of this Section:

“dealing” in relation to property or funds, means receiving, acquiring, transacting, representing, concealing, disposing, converting, transferring or moving, using as security, or providing financial services;

“designated person or entity” means a person or entity designated pursuant to these Regulations or an applicable United Nations Security Council Resolution adopted under Chapter VII of the United Nations Charter;

“designation” or “listing” means the identification of a person, organisation, association or group of persons subject to targeted sanctions pursuant to an applicable United Nations Security Council Resolution;

“delist” means the removal of the name and other identification information of a designated person or entity from the Domestic List or applicable Sanctions List;

“Domestic List” means the list compiled and maintained by the Counter Financing of Terrorism Inter-Ministerial Committee under ;

“economic resources” includes assets of every kind, whether movable or immovable, tangible or intangible, actual or potential, which are not funds and which may be used to obtain funds, goods or services;

“freeze” means to prevent or restrain specific property or funds from being used, transferred, transacted, converted, altered, concealed, moved or disposed of without affecting the ownership thereof;

“person” means a natural person or legal person;

“Resolution” means a resolution of the United Nations Security Council and includes any successor resolution;

“UNSCR 1267” means Resolution 1267 (1999) of the United Nations Security Council and includes its successor resolutions;

“UNSCR 1989” means Resolution 1989 (2011), as amended by Resolution 2253 (2015), and includes its successor resolutions;

“UNSCR 1373” means Resolution 1373 (2001) of the United Nations Security Council and includes its successor resolutions;

“UNSCR 1988” means Resolution 1988 (2011) of the United Nations Security Council and includes its successor resolutions;

“UNSCR 1718” means Resolution 1718 (2006) of the United Nations Security Council and includes its successor resolutions;

“UNSCR 2231” means Resolution 2231 (2015) of the United Nations Security Council and includes its successor resolutions;

“Sanctions Committee” means a Committee of the United Nations Security Council established pursuant to a Resolution of the Security Council;

6.2 Introduction

Targeted Financial Sanctions (TFS) are financial restrictions imposed pursuant to United Nations Security Council Resolutions (UNSCRs) which require the freezing of funds, other assets and economic resources of designated persons and entities and prohibit the making available of funds, financial services or economic resources to such persons and entities. TFS apply to measures relating to the prevention and suppression of terrorism financing and proliferation financing.

6.2.1 The Counter Financing of Terrorism Inter-Ministerial Committee

In Kenya, the Counter Financing of Terrorism Inter-Ministerial Committee (the CFTIMC) is the national inter-agency body responsible for coordinating and overseeing the implementation of TFS related to the financing of terrorism and proliferation financing.

Membership in the CFTIMC comprises representatives from the relevant Government ministries, competent authorities, law enforcement agencies, and other institutions. The FRC acts as the Secretariat to the Committee. Its role is to conduct administrative tasks relating to the work of the Committee including relaying the delisting

Institutions shall comply with the applicable requirements under the following laws and sanctions regimes relating to the freezing of funds and other assets and the prohibition against making funds, assets, economic resources or financial services available to designated persons or entities.

6.3 Targeted Financial Sanctions Related to Terrorism Financing

- (a) the Prevention of Terrorism Act, 2012; and
- (b) the Prevention of Terrorism (Implementation of United Nations Security

Council Resolutions on the Suppression of Terrorism) Regulations (TF Regulations).

6.3.1 Sanctions Regimes on Terrorism Financing

Institutions shall comply with applicable United Nations Security Council sanctions regimes relating to terrorism financing, including:

- (a) **Al-Qaida and ISIL (Da'esh) Sanctions Regime:** UNSCRs 1267/1989/2253, which establishes a targeted sanctions regime against Al-Qaida, ISIL (Da'esh) and associated individuals and entities;
- (b) **Taliban Sanctions Regime:** UNSCR 1988, which establishes a targeted sanctions regime against designated Taliban-associated individuals and entities; and
- (c) **Domestic Designation Regime :** UNSCR 1373, which requires UN member states to establish domestic mechanisms for the designation of persons and entities involved in terrorism and terrorism financing and for the freezing of their funds and other assets without delay.

6.4 Targeted Financial Sanctions Related to Proliferation Financing

Targeted financial sanctions relating to proliferation financing in Kenya are implemented through applicable Kenyan legislation and regulations, including:

- (a) The Prevention of Terrorism Act, 2012.
- (b) The Prevention of Terrorism (Suppression of Proliferation Financing) Regulations.

Institutions shall implement the applicable targeted financial sanctions relating to proliferation financing in accordance with the relevant United Nations Security Council Resolutions and directions issued by the competent authorities.

6.4.1 Sanctions Regimes on Proliferation Financing

Institutions shall comply with applicable United Nations Security Council sanctions regimes relating to proliferation financing, including:

- (b) **Democratic People's Republic of Korea (DPRK) Sanctions Regime:** UNSCR 1718, which establishes targeted financial sanctions against persons and entities designated in connection with the DPRK's proliferation-related activities; and

- (b) **Islamic Republic of Iran Sanctions Regime:** UNSCR 2231 and applicable successor measures, to the extent applicable.

6.5 Policies, Procedures and Systems

Institutions shall establish and maintain appropriate policies, procedures, systems and internal controls to ensure the effective implementation of targeted financial sanctions.

Such policies, procedures and controls shall be consistent with:

- (a) The Prevention of Terrorism Act;
- (b) applicable Regulations;
- (c) applicable United Nations Security Council Resolutions; and
- (d) directives, circulars and guidance issued by the CFIMTC and the FRC and other competent authorities.

6.6 Sanctions Lists

Institutions shall:

- (a) Maintain an up-to-date sanctions List incorporating all applicable UN Security Council sanctions lists and the Domestic List circulated by the FRC.
- (b) institutions may exercise the option of using automated digital subscriptions to maintain up-to-date sanctions lists.

6.7 Consolidated List

The Consolidated List maintained by the United Nations Security Council contains a list of all the individuals and entities designated under the various United Nations Security Council sanctions regimes. The specific sanctions measures applicable to each listed individual or entity are determined by the relevant sanctions regime and the applicable Security Council resolution or decision.

6.8 Designation and Circulation under the International United Nations Security Council Sanctions Regimes

Under the applicable United Nations sanctions regime, the United Nations Security Council or the relevant Sanctions Committee designates, updates or delists persons and entities. The designation, update or delisting is communicated through the established official channels to the Government of Kenya for implementation. Upon receipt, the CFTIMC coordinates the national implementation process and notifies the FRC accordingly. The FRC then circulates the designation, update or delisting to

reporting institutions and issues the instructions to facilitate compliance with the targeted financial sanctions requirements.

6.9 Designation and Circulation under UNSCR 1373 Domestic List

The designation of persons and entities under United Nations Security Council Resolution 1373 (UNSCR 1373) is undertaken through Kenya's domestic designation framework in accordance with the Prevention of Terrorism Act and applicable Regulations. The CFTIMC considers and determines proposals for domestic designation in accordance with the applicable legal framework. Following a designation, the FRC, acting as the Secretariat to the CFTIMC, circulates the relevant designation to reporting institutions and issues the implementation instructions to facilitate the application of the applicable targeted financial sanctions measures.

6.10 Obligations of Institutions Upon Receipt of a Designation, Amendment or Decision

6.10.1 Screening of Customer Database

Upon receipt of a Designation List or update circulated by the FRC, an institution shall, without delay within twenty-four (24) hours:

- (a) Screen its records, databases and business relationships, including inactive and dormant relationships, as applicable, against the Sanctions List;
- (b) Undertake screening whenever an updated Sanctions List is circulated;
- (c) Where an institution identifies a potential match against a Sanctions List, it shall, without delay (within twenty-four (24) hours):
 - (i) take reasonable measures to determine whether the potential match is a true match and eliminate any false positive;
 - (ii) where necessary, obtain additional identification information or documentation from the person or entity concerned or from reliable and independent sources; and
 - (iii) where uncertainty remains, promptly refer the matter to the FRC for guidance.
- (d) An institution shall not treat a person or entity as a designated person solely on the basis of a name similarity where the available information indicates that the person or entity is not the designated person or entity

6.10.2 Freezing of Funds and Other Assets

- (a) Where an institution confirms a positive match with a designated person or entity, it shall, without delay (within twenty-four (24) hours and without prior notice:
 - (i) freeze all funds and other assets that are owned or controlled, directly or indirectly, by the designated person or entity;
 - (ii) freeze funds and other assets that are jointly owned or controlled by the designated person or entity;
 - (iii) freeze funds and other assets derived or generated from funds or other assets owned or controlled, directly or indirectly, by the designated person or entity; and
 - (iv) freeze funds and other assets of persons or entities acting on behalf of, or at the direction of, the designated person or entity.

6.11 Prohibition on making frozen funds available to a designated person or entity

An institution shall not make available, directly or indirectly, any funds, other assets, economic resources or financial or related services to or for the benefit of a designated person or entity, except where permitted by applicable law or expressly authorised by the CFTIMC.

6.12 False Positives

In cases where a person or entity whose funds or other assets have inadvertently been frozen, or who has otherwise been affected by sanctions measures, due to a name or other identifying information matching or resembling that of a designated person or entity on a sanctions list may apply to the relevant UNSCR Sanctions Committee or CFTIMC for a determination that they are not the designated person or entity.

Where the Committee determines that the applicant is not the designated person or entity, it shall communicate its decision to the relevant persons and provide guidance on the unfreezing of the applicant's funds or other assets.

6.13 Delisting

Where a person or entity is removed from a United Nations sanctions list, the relevant United Nations Sanctions Committee shall communicate the delisting through the established official channels to the Government of Kenya. The CFTIMC shall notify

the FRC of the delisting. The FRC shall promptly notify institutions of the delisting and provide appropriate guidance on the required unfreezing and related actions.

6.13.1 Actions to be taken by Institutions upon Notification of Delisting

Upon notification by the FRC of a delisting, an institution holding funds or other assets of the delisted person or entity shall, without delay:

- (a) unfreeze the funds or other assets affected by the delisting, to the extent applicable;
- (b) update its sanctions screening systems and internal records;
- (c) remove the person or entity from its internal sanctions lists, where applicable; and
- (d) retain records of the actions taken.

6.14 Authorisation to Access Funds or Other Assets Subject to Freezing Measures

Where funds or other assets have been frozen pursuant to a designation under an applicable United Nations sanctions regime or the Domestic List, such funds or other assets shall remain frozen unless and until the institution receives an applicable authorisation or decision from the competent authority, through the FRC, permitting access to or release of the funds or other assets. A designated person or entity may apply for authorisation to access frozen funds or other assets where permitted under the applicable United Nations Security Council Resolution or through CFTMC.

Such access may include, where authorised, funds required for:

- (a) basic expenses necessary for the satisfaction of basic needs, including food, rent or mortgage payments, medicines and medical treatment, taxes, insurance premiums and public utility charges;
- (b) reasonable professional fees and expenses associated with the provision of legal services; and
- (c) fees or service charges associated with the maintenance or management of frozen funds or other assets.

6.14.1 Actions to be taken upon receipt of Authorisation to access or release funds from UNSCR Sanctions Committee or the CFTMC

Upon receipt of an authorisation to unfreeze funds or other assets from the FRC, an institution shall:

- (a) Permit access to or release funds or other assets only to the extent specified in the authorisation.

- (b) Maintain records of the authorisation, funds or other assets released and actions taken pursuant to the authorisation.

6.15 Third-Party Claims

Where the relevant United Nations Sanctions Committee or the CFTIMC has determined that a third-party bona-fide claim in respect of frozen funds or other assets is valid and has authorised or directed the release or unfreezing of such funds or other assets, the FRC shall communicate the decision to the relevant financial institution that has frozen the assets.

A bona-fide third party claims refers where innocent, unrelated parties who have a legitimate, good-faith legal or financial interest in assets that have been frozen under a sanctions regime. This is because sanctioned persons or entities often mix their funds with legitimate businesses or transfer properties to obscure ownership, innocent third parties can accidentally have their assets frozen.

Upon communication of the decision by the FRC directing the institution to unfreeze the fund or other assets of the third party, the institution shall, without delay:

- (a) Release or unfreeze the funds or other assets to the extent specified in the decision;
- (b) Ensure that only the funds or other assets covered by the decision are released or unfrozen;
- (c) Continue to freeze any funds or other assets that remain subject to the applicable targeted financial sanctions;
- (d) Maintain records of the decision received and the action taken to implement
- (e) Provide confirmation of implementation to the FRC where required.
- (f) An institution shall not release or otherwise deal with frozen funds or other assets solely on the basis of a third-party claim. Release or unfreezing of assets shall only be undertaken pursuant to a decision or authorisation that has been by a UNSRC Sanctions Committee or the CFTIMC through the FRC through the FRC.

6.16 Reporting Obligations Targeted Financial Sanctions

6.16.1 Return

An institution shall, within twenty-four (24) hours of taking action to freeze or unfreeze funds or other assets pursuant to a targeted financial sanctions designation or delisting, submit a return to the CFTIMC through the FRC, in the format

specified by the FRC.

The return shall include, as applicable:

- (a) the account number;
- (b) the name of the account holder;
- (c) the date and time of the freezing or unfreezing;
- (d) the balance of the account at the time of freezing or unfreezing; and
- (e) details of related accounts and the balances in those accounts.

6.16.2 Suspicious Transaction Reports Related to Targeted Financial Sanctions

- (a) An institution shall submit a Suspicious Transaction Report to the FRC within twenty-four (24) hours of identifying:
 - (i) a positive name match and taking the required action under this Section;
 - (ii) an attempted transaction involving a designated person or entity;
 - (iii) an attempted transaction involving a person or entity owned or controlled, directly or indirectly, by a designated person or entity;
 - (iv) an attempted transaction involving a person or entity acting on behalf of, or at the direction of, a designated person or entity; or
 - (v) any actual or attempted activity that appears intended to evade or circumvent targeted financial sanctions or applicable freezing and prohibition requirements.
- (b) The STR shall include relevant information concerning the designated person or entity, the funds or other assets involved and the measures taken by the institution.

6.17 Record Keeping

Institutions shall maintain comprehensive records relating to compliance with targeted financial sanctions for a minimum period of seven (7) years.

Records shall include:

- (a) sanctions lists received and implemented;
- (b) screening results, including positive matches and false positives;
- (c) frozen funds, other assets and economic resources;
- (d) STRs submitted to the FRC;
- (e) delisting and unfreezing actions;
- (f) authorisations and decisions received from the CFMTC; and
- (g) internal decisions, approvals and supporting documentation relating to TFS

6.18 Ongoing Sanctions Screening and Monitoring

Institutions shall:

- (a) Regularly review the United Nations Consolidated List and the Domestic List and conduct ongoing monitoring of relevant business relationships and transactions to identify and mitigate the risk of terrorism financing and proliferation financing.
- (b) Ensure that their sanctions screening systems are updated promptly following any addition, amendment or delisting communicated by the FRC.
- (c) Institutions may opt to utilize digital subscriptions to facilitate monitoring and screening.

6.19 Country- Specific United Nations Security Council Resolutions Sanctions Regimes Arising from Threats to International Peace and Security

The United Nations Security Council (UNSC) from time to time, adopts country specific resolutions in response to war, armed conflict, civil strife, terrorism, or threats to international peace and security. Such resolutions may impose sanctions and other restrictive measures, including targeted financial sanctions, asset freezes, travel bans, arms embargoes, and restrictions on the provision of financial services.

Examples of these UN Security Council Resolutions include:

- **UNSCR 1518 Sanctions List (Iraq):** Established to locate and freeze assets belonging to individuals and entities associated with the former Saddam Hussein regime.
- **UNSCR 1591 Sanctions List (Sudan):** Targets individuals impeding the peace process, committing human rights violations, or violating the arms embargo in Darfur.
- **UNSCR 1533 Sanctions List (Democratic Republic of the Congo):** Targets individuals and entities violating arms embargoes, recruiting child soldiers, or committing human rights violations in the DRC.
- **UNSCR 1970 Sanctions List (Libya):** Focuses on individuals threatening the peace, stability, or security of Libya, or involved in human rights abuses.
- **UNSCR 2140 Sanctions List (Yemen):** Targets those engaging in or providing support for acts that threaten the peace, security, or stability of Yemen.
- **UNSCR 2206 Sanctions List (South Sudan):** Focuses on those responsible for actions or policies that threaten the peace, security, or stability of South Sudan.
- **UNSCR 2653 Sanctions List (Haiti):** Targets individuals and entities engaging

in or supporting gang violence, criminal activities, or human rights abuses destabilizing Haiti.

- **2127 Sanctions List (Central African Republic):** Focuses on individuals and entities violating the arms embargo or committing atrocities in the CAR.
- **2048 Sanctions List (Guinea-Bissau):** Targets those seeking to prevent the restoration of constitutional order or involved in the 2012 coup d'état.

Institutions shall take immediate steps to implement applicable United Nations Security Council Resolutions and related measures designated under Kenyan law. In particular, institutions shall, where applicable:

- (a) identify any designated individual or entity;
- (b) identify any funds, financial assets and economic resources belonging to, or owned or controlled, directly or indirectly, by designated individuals or entities, including those held by any other person or entity on their behalf;
- (c) freeze, without delay, any funds, financial assets and economic resources owned or controlled, directly or indirectly, by designated individuals or entities, or by persons acting on their behalf;
- (d) identify any Kenyan national or person in Kenya who has availed, directly or indirectly, any funds, financial assets or economic resources to a designated individual or entity;
- (e) refrain from making available, directly or indirectly, any funds, financial assets or economic resources to, or for the benefit of, designated individuals or entities, except as permitted under applicable law;
- (f) promptly report or communicate any action taken pursuant to the applicable United Nations Security Council Resolution to the CFTIMC, and
- (g) maintain appropriate records of actions taken in implementing the applicable United Nations Security Council Resolutions.

PART VII: SPECIAL CONSIDERATIONS FOR INSTITUTIONS ONBOARDING VIRTUAL ASSET SERVICE PROVIDERS (VASPs) AS CUSTOMERS

7.1 Definitions

“anonymity-enhancing services” means offering, facilitating or executing transactions in digital assets, with the effect or intention of concealing information;

“custodial wallet” means a wallet in which the private keys to the subject's virtual assets are held and managed by a third party for proof of ownership and facilitation of transactions;

“distributed ledger technology” means a decentralized digital system for recording transactions where the data is simultaneously shared, replicated, and synchronized across computer networks;

“fiat currency” means currency that is issued by the relevant body in a country or by government, that is designated as a legal tender in its country of issuance through legislation;

“issuer” means a person who is authorised to issue a virtual asset offering under this The Virtual Service Providers Act;

“licence” means a virtual asset service provider licence granted under the Virtual Asset Service Providers Act;

“licensee” means a legal person licensed to operate as a virtual asset service provider conducting one or more permissible activities under the Virtual Asset this Act; Service Providers Act;

7.2 Introduction

Under the Kenya’s AML/CFT/CPF legal framework, Virtual Asset Service Providers (VASPs) are reporting institutions and are subject to the applicable preventive measures under the Proceeds of Crime and Anti-Money Laundering Act (POCAMLA), the Proceeds of Crime and Anti-Money Laundering Regulations and other applicable AML/CFT/CPF laws and regulations.

The Virtual Asset Service Providers Act, 2025 and the Virtual Asset Service Providers Regulations, 2026 establish a licensing, regulatory and supervisory framework for VASPs operating in or from Kenya. The framework also provides for specific obligations relating to, among other matters, customer due diligence, record keeping, governance, compliance, safeguarding of customer assets, technology, outsourcing, transaction monitoring and cooperation with competent authorities.

Accordingly, when onboarding a VASP as a customer, an institution may consider not only the VASP's ML/TF/PF risk profile, but also VASP-specific compliance matters arising from the nature of virtual asset activities and the regulatory obligations applicable to VASPs.

The factors highlighted in this Part are intended to identify matters that may be relevant to the institution's customer acceptance and due diligence processes because the prospective customer is a VASP. They are not intended to create

additional obligations for VASPs beyond those imposed by applicable law or to constitute a separate risk-rating methodology.

The relevance of individual factors may vary according to the type of virtual asset services provided by the VASP, the scope of its licence, its business model and the nature of the proposed relationship with the institution.

7.3 Applicable laws and regulations

Institutions shall consider the relevant laws and regulations governing the operations of VASPs and the applicable AML/CFT/CPF requirements under Kenya's AML/CFT/CPF laws and regulations.

This includes:

- (a) The Virtual Asset Service Providers Act, 2025;
- (b) The Virtual Asset Service Providers Regulations, 2026;
- (c) The Proceeds of Crime and Anti-Money Laundering Act (POCAMLA);
- (d) The Proceeds of Crime and Anti-Money Laundering Regulations (POCAMLA) Regulations);;
- (e) The Prevention of Terrorism Act,(POTA)
- (f) The Banking Act
- (g) The National Payments System Act.
- (h) The Capital Markets Authority Act.

7.4 Areas of Consideration

7.4.1 Licensing and Regulatory Framework

- Verify that the VASP is licensed in accordance with the licensing requirements under the Virtual Assets Services Providers Act. The licensing authorities governing the licensing of VASPs are the Central Bank of Kenya (CBK) and the Capital Markets Authority (CMA).
- Note that under the VASPs Regulations, offshore platforms targeting Kenyan consumers or deriving economic benefit from Kenya are legally deemed to be operating within the country and must obtain a license, regardless of whether they have a local office.
- Dependent of the activities or services that the VASPs will be offering. A VASP can be subject to:
 - (i) Single licensing regime under Central Bank of Kenya (CBK).

- (ii) Single licensing under CMA (Capital Markets Authority).
- (iii) Dual licensing regime under both the CBK and CMA.
- Understand the VASP's business model including its operational structure, target customer demographic, transaction flows, and underlying technology infrastructure.
- Verify that the specific license(s) held by the VASP explicitly authorize the specific services and transaction types intended to be routed through the VASP's bank accounts.
- Confirm that all activities undertaken by the VASP are strictly permissible services under the relevant license(s) for which it has been formally in accordance with the First Schedule of the Virtual Asset Service Providers Act.
- Establish whether the institution possesses the requisite technical infrastructure, monitoring tools, and risk management capacity to effectively support and oversee the proposed activities of the VASP.
- Establish whether the VASP is subject to AML/CFT/CPF supervision and has registered with the FRC as a reporting institution in line with the requirement of POCAMLA for reporting institutions that are financial institutions.

7.4.2 Customer Due Diligence (CDD)

- Consider whether the VASP has appropriate procedures for preventing the use of mixer or tumbler services or anonymity-enhancing services.
- Consider whether the VASP maintains sufficient records to link virtual asset transactions, including transaction identification numbers and wallet addresses, to the relevant customer's KYC information and other transaction details, and whether such records are retained for the required period.

7.4.3 Record-Keeping

- Evaluate the VASP's capability to link customer identity profiles and Know Your Customer (KYC) information with relevant blockchain wallet addresses and transactions.
- Ensure that the VASP is capable of retrieving and providing complete transaction records, transaction identifiers, relevant wallet addresses and other information necessary to enable the institution to understand and monitor the source and destination of funds.
- Assess whether the VASP is capable of providing relevant customer and transaction information promptly in response to a request from competent authorities such as a regulatory, supervisory or law enforcement authority.
- Confirm that the VASP records retention policy requires that all transaction

records in accordance with the record-keeping requirements prescribed under the, POCAMLA and other applicable legal and regulatory requirements. not less than seven years from the date of the transaction.

7.4.4 Politically Exposed Persons (PEPs)

- Screen the VASP's beneficial owners, founders, directors, senior management and other relevant persons for PEP status.
- Assess the effectiveness of the VASP's internal PEP screening systems to ensure that the VASP appropriately identifies, assesses and manages PEP relationships within its customer base.
- Verify that the VASP applies enhanced measures, including obtaining and establishing the source of wealth and source of funds, and obtains appropriate senior management approval before establishing or continuing relationships with PEPs, where required under applicable law and regulatory requirements.

7.4.5 Nested Relationships

- Identify and assess “nested” arrangements where an unregulated or inadequately regulated downstream virtual exchange or other virtual asset business uses the infrastructure or accounts of the onboarded VASP to access the banking system.
- Identify and appropriately manage relationships where the VASP provides indirect access to financial services to un-vetted or inadequately assessed third-party financial institutions, VASPs or other virtual asset businesses. Ir
- Identify and appropriately manage relationships where VASPs, particularly brokers provide direct or indirect access to virtual asset financial services.
- Verify that the VASP conducts appropriate due diligence on the AML/CFT/CPF controls of VASPs and other institutional partners with which it maintains business relationships, particularly given that virtual transactions are deemed to be cross-border transactions.

7.4.6 New Technologies

- Evaluate the VASP's framework for assessing ML/TF/PF and other financial crime risks before the introduction of new virtual assets, tokens, protocol integrations or smart contract functionalities among others.
- Consider whether the VASP has appropriate systems, policies and controls to manage the technologies it uses to provide virtual asset services, including appropriate oversight and management of technology-related risks.

7.4.7 Wire Transfers

- Verify that the VASP has implemented technology capable of securely transmitting and receiving the originator and beneficiary information required under applicable law and regulatory requirements for virtual asset transfers.
- Ensure that the VASP can demonstrate that it has appropriate systems and procedures to hold, reject or subject non-compliant transfers to further review, as appropriate.
- Ensure that the VASP performs appropriate due diligence and risk assessments on counterparty VASPs and other relevant counterparties to which it sends or from which it receives virtual assets.
- Where the VASP outsources its customer identification, verification or screening processes to a third-party vendor or software application, the institution must assess the VASP's due diligence and ongoing oversight of that third party, including the reliability and adequacy of its data verification standards.

7.4.8 Internal Controls and Foreign Operations

- Assess whether the VASP has access to appropriate blockchain analytics and forensic capabilities, proportionate to the nature, scale and complexity of its activities and risk profile. Such capabilities may include blockchain transaction monitoring, wallet screening and transaction risk assessment tools.
- Where the VASP operates across multiple jurisdictions, the must assess whether the VASP applies appropriate group-wide AML/CFT/CPF standards across its operations, taking into account applicable local legal and regulatory requirements.

7.4.9 Compliance Function

Verify that the VASP has appointed or designated a compliance officer to monitor compliance with the AML/CFT/CPF regulatory requirements.

7.4.10 Internal Audit Function

- Verify that the VASP maintains an appropriately independent and adequately resourced audit or assurance function capable of assessing the effectiveness of its AML/CFT/CPF framework and transaction monitoring systems.

7.4.11 Higher-Risk Countries

- Ensure that VASPs registered, incorporated or operating in jurisdictions

presenting heightened ML/TF/PF risks to enhanced scrutiny. Particular attention should be given to VASPs with or no substantive presence in their jurisdiction of incorporation or which conduct significant business through jurisdictions presenting heightened risks.

- Take into account applicable FATF statements concerning jurisdictions under increased monitoring or subject to a call for action, together with applicable Kenyan laws and regulatory requirements.
- The VASP applies proportionate enhanced due diligence to transaction flows originating from or directed towards higher-risk jurisdictions, where warranted by the risk assessment and applicable legal and regulatory requirements.

7.4.12 Reporting of Suspicious Transactions

- The VASP manages internal alerts and whether it maintains clear procedures for identifying, escalating and investigating transactions linked to high-risk activities, including darknet markets, ransomware, theft of virtual assets, fraud, mixer or tumbler services and other indicators of illicit activity.
- The VASP's internal escalation procedures to ensure that Suspicious Transaction Reports (STRs) are submitted promptly to the (FRC within 48 hours.
- The VASP has robust internal controls to prevent employees, officers, agents and other relevant persons from tipping off customers whose transactions or accounts are subject to investigation or reporting.

PART VIII: RETURNS

Institutions shall submit all AML/CFT/CPF returns and related regulatory reports required by the CBK within the stipulated timelines, or such other timelines as may be prescribed by the CBK from time to time.

PART IX: REMEDIAL MEASURES

Central Bank may pursue any or all remedial actions provided under sections 33, 33A, 33D 34 and 55 of the Banking Act.

PART X: EFFECTIVE DATE

10.1 **Effective Date** - The effective date of these guidelines shall be

10.2 **Supersedence** - This guideline supersedes the Guideline on Anti-Money Laundering and Combating the Proceeds of Crime that was issued on January 1, 2013.

PART X: ENQUIRIES

Enquiries on any aspect of this guideline should be referred to:

Director,

Bank Supervision Department

Central Bank of Kenya

P.O. Box 60000 - 00200

NAIROBI

TEL. 2860000 e-mail : fin@centralbank.go.ke

MONEY LAUNDERING, TERRORISM FINANCING AND PROLIFERATION FINANCING

Money Laundering

Money laundering techniques continue to evolve in response to advances in technology, changes in financial services, and measures implemented to combat financial crime. Although money laundering may be undertaken using a wide variety of methods, the laundering process generally comprises three stages. These stages may occur separately, simultaneously, or overlap depending on the laundering method employed.

(i) Placement

Placement is the physical introduction or disposal of proceeds derived from criminal activity into the financial system.

At this stage, criminals attempt to move illicit proceeds away from their source by depositing cash into financial institutions, purchasing monetary instruments, or converting cash into other assets.

(ii) Layering

Layering involves separating illicit proceeds from their criminal origin by creating complex layers of financial transactions designed to disguise the audit trail and conceal the ownership and source of the funds. Layering may involve numerous transfers between accounts, jurisdictions, products or entities to make tracing the proceeds more difficult.

(iii) Integration

Integration is the process through which laundered funds are reintroduced into the legitimate economy so that they appear to originate from lawful activities. the placement and layering stages are successful, integration enables criminals to enjoy the proceeds of crime while concealing their illicit origin.

Understanding these stages assists financial institutions in identifying suspicious transactions and implementing appropriate preventive measures. Financial institutions should therefore maintain ongoing vigilance throughout the customer relationship and monitor transactions for money laundering indicators.

ML/TF/PF Vulnerabilities

2.1 Money Laundering Vulnerabilities

Money laundering risks may arise where criminals exploit weaknesses in the financial system, including:

- cash-based transactions;
 - cross-border movement of funds;
 - complex transactions or intermediaries used to conceal ownership or source of funds; and
- transactions without a clear lawful or economic purpose.

2.2 Terrorism Financing Vulnerabilities

Terrorism financing risks may arise from weaknesses in financial systems and controls, including:

- ineffective AML/CFT/CPF frameworks and targeted financial sanctions;
- inadequate supervision and CDD;
- reliance on cash or informal financial channels;
- Ltd. beneficial ownership transparency; and
- exposure to higher-risk jurisdictions.

2.3 Proliferation Financing Vulnerabilities

Proliferation financing risks may arise where controls over financial activities and trade are inadequate, including:

- weak implementation of targeted financial sanctions;
- illicit trade networks;
- inadequate enforcement measures; and
- transactions involving dual-use goods or materials that may have both legitimate and proliferation-related purposes.

DETERMINING BENEFICIAL OWNERSHIP OF LEGAL PERSONS AND LEGAL ARRANGEMENTS

1. General Principles

- (a) A beneficial owner shall be a natural person who ultimately owns or controls a legal person or legal arrangement.
- (b) In determining beneficial ownership, an institution shall consider:
 - (i) direct and indirect ownership;
 - (ii) voting rights;
 - (iii) rights to appoint or remove directors, partners or managers;
 - (iv) significant influence or significant control; and
 - (v) any other means through which a natural person ultimately owns or controls the customer.
 - (vi) A beneficial owner is a natural person who holds at least 10% of issued shares or voting rights, holds the right to appoint or remove a director, or exercises significant influence or control over the company

2. Determination of the Beneficial Owner

The Companies (Beneficial Ownership Information) Regulations, define the beneficial owner as the natural person who satisfies the following criteria:

- (a) Holds at least 10% of the issued shares in the company either directly or indirectly
- (b) Exercises at least 10% of the voting rights in the company either directly or indirectly
- (c) Holds a right, directly or indirectly, to appoint or remove a director of the company
- (d) Exercises significant influence or control, directly or indirectly, over the company

Highlighted below are examples/scenarios of how beneficial ownership is determined:

Examples:

i. Legal Person: Kwaheri Ltd.

Scenario : Corporate Ownership Chain

Corporate shareholder: Uzuri Ltd. holds 40 per cent of Kwaheri Ltd..

Shareholders of Uzuri Ltd.:

Joy M. – 30 per cent; and
Michael O. – 20 per cent.

Where appropriate, indirect ownership may be calculated by multiplying the ownership percentages at each level:

Joy M.: $30\% \times 40\% = 12\%$

Joy M. therefore has an indirect ownership interest of 12 per cent in Kwaheri Ltd. and meets the applicable 10 per cent ownership threshold.

Michael O.: $20\% \times 40\% = 8\%$

Michael O. therefore has an indirect ownership interest of 8 per cent in Kwaheri Ltd. does not meet the 10 per cent threshold on the basis of ownership alone.

- (a) The institution shall nevertheless assess whether Michael O. exercises beneficial ownership through voting rights, significant influence or significant control.
- (b) Where a natural person has interests through more than one ownership chain, the interests shall be considered cumulatively, where applicable.

ii. Legal Arrangement – Maisha Family Trust

Scenario: Trust Ownership

Shareholder: Maisha Family Trust holds 20 per cent of Kizungu Ltd.

Trust parties:

Settlor – David N.;

Trustee – Pesa Trust Corporate Services Ltd.;

Protector – Anne K.; and

Beneficiaries – Tony N. and Susan N.

The trust deed provides for Tony N. to have a 60 per cent vested beneficial interest and Susan N. a 40 per cent vested beneficial interest.

Where the nature and terms of the trust permit the beneficiary's interest to be attributed to the trust's shareholding, an institution may use the following calculation as an illustration:

Tony N. $60\% \times 20\% = 12\%$

Susan N. $40\% \times 20\% = 8\%$

- (a) Tony N. therefore meets the 10 per cent threshold on that basis, while Susan N. does not meet the threshold on that basis alone.
- (b) The institution shall nevertheless assess the powers and interests of the settlor, trustee, protector and beneficiaries to determine whether any of them exercises ultimate effective control or significant influence.
- (c) The calculation above is provided as an example and is not a Universal formula to be applied mechanically to all trusts. The institution shall have regard to the trust deed and the nature of the rights and powers held by the relevant persons.

iii. Company Ltd. by Guarantee - Tumaini Foundation, a company Ltd. by guarantee.

Scenario : Voting Rights and Control

The members hold voting rights as follows:

Amina K. – 35 per cent;
 Brian M. – 25 per cent;
 Charity O. – 20 per cent; and
 Daniel P. – 20 per cent.

- (a) As a company limited by guarantee does not have issued shares in the same manner as a company Ltd. by shares, the institution shall consider voting rights and other means of control.
- (b) In this example, each member holds more than 10 per cent of the voting rights and shall therefore be identified as a beneficial owner.
- (c) The institution shall also consider whether any other natural person exercises significant influence or control, including through rights to appoint or remove directors or other relevant powers.

iv. Ltd. Liability Partnership – Imara Consulting LLP.

Scenario: Direct and Indirect Ownership

The partners are:

Horizon Holdings Ltd. – 40 per cent of capital contribution and profits;
 Joseph N. – 30 per cent; and
 Mary W. – 30 per cent.

Horizon Holdings Ltd. is owned by:

Peter K. – 60 per cent; and
Sarah T. – 40 per cent.

Joseph N. and Mary W. each hold 30 per cent of the capital contribution and profits and therefore meet the applicable threshold.

The institution shall look through Horizon Holdings Ltd.:

Peter K.: $60\% \times 40\% = 24\%$

Sarah T.: $40\% \times 40\% = 16\%$

Both Peter K. and Sarah T. therefore meet the applicable threshold on the basis of their indirect interests.

The institution shall also consider voting rights, rights to appoint or remove partners or managers, significant influence or significant control and nominee arrangements.

v. Where Ownership Does Not Establish Beneficial Ownership

- (a) An institution shall not conclude that a person is not a beneficial owner solely because the person's ownership interest is below the applicable threshold.
- (b) The institution shall assess whether the person exercises control or significant influence through other means.
- (c) Where no natural person can be identified through ownership or control, the institution shall identify the senior managing official in accordance with the applicable beneficial ownership requirements.

3. Documentation

- (a) An institution shall document the basis for its beneficial ownership determination, including the ownership and control structure, the natural person or persons identified, and the documents, data or information relied upon.
- (b) Where no beneficial owner can be identified through ownership or control, the institution shall document the steps undertaken and the basis for identifying the senior managing official.

4. Reference to Business Registration Service Guidance

Institutions may refer to guidance and other relevant materials issued by the Business Registration Service (BRS) when determining and verifying beneficial ownership information. Such guidance shall be read together with the applicable legislation and regulations in force.

INDICATORS OF SUSPICIOUS TRANSACTIONS

The following are examples of transactions or activities that may give rise to suspicion and warrant further review and, where appropriate, submission of an STR to the FRC:

- Large or frequent cash deposits, withdrawals or transfers that are inconsistent with the customer's known profile, business, income or source of funds.
- Multiple transactions structured below applicable reporting thresholds or otherwise arranged to avoid detection or reporting.
- Rapid movement of funds through an account, including funds received and transferred shortly thereafter without an apparent legitimate purpose.
- Significant or repeated third-party payments, particularly where the relationship between the parties or the purpose of the payments cannot be reasonably established.
- Transactions involving multiple accounts, persons or entities that appear designed to conceal the source, ownership or destination of funds.
- Significant cross-border transactions involving jurisdictions with which the customer has no apparent legitimate connection or jurisdictions presenting heightened ML/TF/PF risks.
- Transactions involving shell companies, complex ownership structures or entities with little or no apparent legitimate economic activity.
- Transactions inconsistent with the customer's stated business, occupation, expected activity or established transaction pattern.
- Transactions involving persons or entities known or reasonably suspected to be involved in criminal activity, terrorism financing, proliferation financing or other illicit activity.
- Transactions involving designated persons or entities, or transactions that appear intended to circumvent or evade targeted financial sanctions.
- Transactions involving persons or entities acting on behalf of, or at the direction of, designated persons or entities.
- Attempts to transfer, withdraw or otherwise deal with frozen funds or assets, or other activity indicating an attempt to circumvent targeted financial sanctions.
- Transactions involving high-risk virtual asset activities, including transfers to or from VASPs, virtual asset wallets, mixers, tumblers or anonymous-enhancing technologies where the source, destination or purpose cannot reasonably be established.
- Transactions involving virtual asset wallets, platforms or service providers associated with fraud, ransomware, theft, darknet markets, sanctions evasion or other illicit activity.

- Multiple transactions that individually appear legitimate but, when considered collectively, demonstrate an unusual or unexplained pattern.
- A customer who is unable or unwilling to provide credible information or supporting documentation concerning the source, destination or purpose of funds.
- Repeatedly changing or contradictory explanations concerning the source or purpose of funds or transactions.
- An attempted transaction that is abandoned after the institution requests additional CDD information or supporting documentation, where the circumstances give rise to suspicion.
- Any other transaction or activity that has no apparent economic or lawful purpose or that gives rise to a reasonable suspicion of money laundering, terrorism financing, proliferation financing or proceeds of crime.

3.2 Consider Cumulative and Pattern-Based Suspicious transactions

Institutions should not assess transactions in isolation. Suspicion may arise from the cumulative effect of several transactions, accounts, customers or relationships, even where individual transactions do not appear unusual.

Institutions should therefore consider:

- The frequency, volume, value and pattern of transactions over time.
- Transactions across multiple accounts held by the same customer or related persons.
- Transactions involving apparently unrelated customers that demonstrate common beneficiaries, counterparties, addresses, telephone numbers or other connections.
- Transactions conducted across different branches or channels.
- The relationship between incoming and outgoing funds.
- Changes in transaction patterns following customer onboarding or changes in ownership or control.
- The customer's explanations and whether they are consistent with available information.
- Whether the transactions are consistent with the customer's known business, occupation, source of wealth and source of funds.
- Whether the overall activity has an apparent economic or lawful purpose.
- Institutions should consider the nature, frequency, value and pattern of cash transactions, rather than relying solely on transaction thresholds, when assessing ML/TF/PF risks.

The Role of Financial Institutions in the Identification and Monitoring of Large Cash Transactions by Financial Institutions

4.1 Systems and Controls

Financial institutions should maintain appropriate systems and controls to identify and monitor cash transactions, including:

- (a) Large cash deposits and withdrawals.
- (b) Frequent cash transactions that are inconsistent with the customer's known business, occupation or expected account activity.
- (c) Multiple cash transactions conducted within a short period.
- (d) Transactions involving several accounts or persons that appear to be structured to avoid reporting or monitoring requirements.
- (e) Cash transactions that are inconsistent with the customer's known source of funds or source of wealth.
- (f) Cash transactions involving customers, sectors, jurisdictions or activities presenting heightened ML/TF/PF risks.

4.2 Structuring of Cash Transactions

- Financial institutions should identify and investigate transactions that may indicate structuring or other attempts to circumvent applicable reporting requirements.
- Particular attention should be given to repeated cash deposits or withdrawals that are individually below the reporting threshold but, when considered collectively, are significant or inconsistent with the customer's expected activity.
- Where such activity gives rise to suspicion, the institution shall comply with the applicable suspicious transaction or activity reporting requirements.

4.3 Source of Funds

Financial institutions should apply appropriate CDD measures to cash transactions and, where warranted by the risk, establish the source and intended purpose of the funds. The institution should consider whether the cash activity is consistent with:

- the customer's profile and occupation or business;
- the customer's expected account activity;
- the customer's source of funds and source of wealth, where applicable;
- the nature and location of the customer's business; and
- the customer's geographical and other relevant ML/TF/PF risk factors.

- Where the information obtained is inconsistent with the customer's profile or does not satisfactorily explain the transaction, the institution should undertake further enquiries and apply enhanced due diligence where appropriate.

4.4 Cash Transactions by Non-Customers

Financial institutions should maintain appropriate controls over cash transactions conducted by persons who are not customers of the institution. Such controls should enable the institution to identify the person conducting the transaction, understand the purpose of the transaction and assess the associated ML/TF/PF risks.

4.5 Suspicious Cash Transactions

- A cash transaction that meets the reporting threshold is not necessarily a suspicious transaction. Conversely, a cash transaction below the reporting threshold may give rise to suspicion.
- Where a financial institution knows or reasonably suspects that a cash transaction or related activity may involve proceeds of crime, money laundering, terrorism financing or proliferation financing, it shall comply with the applicable requirements for reporting suspicious transactions or activities to the FRC.

The institution should consider the transaction together with the customer's other transactions and relevant customer information when determining whether a suspicion arises.

4.6 Record-Keeping

- Financial institutions shall maintain adequate records of cash transactions, including records supporting customer identification, transaction details, enquiries undertaken, decisions made and reports submitted to the FRC.
- Records shall be maintained for a minimum of seven years as prescribed under POCAMLA and the POCAMLA Regulations and shall be readily retrievable for examination by the FRC or other competent authorities.

4.7 Governance and Internal Controls

- Financial institutions should establish clear procedures for the identification, monitoring, escalation and reporting of cash transactions.
- The procedures should clearly define the responsibilities of relevant business units, compliance personnel and the Money Laundering Reporting Officer (MLRO).
- Institutions should periodically assess the effectiveness of their cash transaction controls and update them to address emerging ML/TF/PF risks and changes in applicable legal and

- regulatory requirements.

4.8 Risk-Based Approach

- The application of cash transaction controls should be proportionate to the institution's risk profile and the risks presented by its customers, products, services, delivery channels and geographical areas.

