

BANKI
KUU YA
KENYA



CENTRAL
BANK OF
KENYA

Haile Selassie Avenue
P.O. Box 60000 - 00200 Nairobi, Kenya
Telephone: 2860000, Fax: 3340192

November 3, 2023

BANKING CIRCULAR NO. 14 OF 2023

**TO ALL CHIEF EXECUTIVE OFFICERS OF COMMERCIAL BANKS,
MORTGAGE FINANCE COMPANIES AND MICROFINANCE BANKS**

**AML/CFT/CPF OBLIGATIONS ON CUSTOMER DUE DILIGENCE, ENHANCED
DUE DILIGENCE AND RECORD KEEPING**

1.0 BACKGROUND

Kenya continues to take measures to strengthen its anti-money laundering (AML), countering the financing of terrorism (CFT) and countering the financing of proliferation (CPF) regime. To this end, the AML/CFT/CPF legal and regulatory frameworks have been revised to align them with Financial Action Task Force (FATF) AML/CFT/CPF Standards. This has been done through the AML/CFT (Amendment) Act, 2023, Proceeds of Crime and Ant-Money Laundering Regulations, 2023 and Prevention of Terrorism (Implementation of the United Nations Security Council Resolutions on Suppression of Terrorism) Regulations, 2023.

Kenya went through a mutual evaluation of its anti-money laundering and combating of terrorism financing and countering proliferation financing (AML/CFT/CPF) regime by the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG) from October 2021 to July 2022. The mutual evaluation report (MER) for Kenya was adopted by the ESAAMLG at its plenary meeting in Livingstone, Zambia and published in September 2022. The Report noted some deficiencies relating to customer due diligence (CDD), enhanced due diligence (EDD) and record keeping. CDD and record keeping are pivotal requirements within the FATF requirements and should be given due attention by supervisors and financial institutions.

The Central Bank of Kenya (CBK) issues this Circular to remind financial institutions of their AML/CFT/CPF obligations relating to CDD, EDD and record keeping. This Circular supplement other circulars issued by the CBK in the past relating to CDD especially the Circular on Beneficial Ownership information.

2.0 CUSTOMER DUE DILIGENCE

Institutions should apply basic CDD to customers as provided for under the law. As part of the on-boarding process, institutions should obtain original copies of identification documents from which copies can be produced for retention by the institution. The identity of customers should be verified using independent sources. Verification of information supplied by foreigners should be performed notwithstanding the challenges for some institutions in having direct access to independent reliable sources for verification. Any change in customer risk profile should form a basis for reviewing the customer's CDD.

BO identification and verification is critical as part of CDD. It is noted that some institutions have challenges understanding the nature of BO information. Placing reliance on declarations made by customers may sometimes be inconclusive as to the true identity of a BO. Institutions should therefore use such declarations as a basis to investigate further the true identity of a BO.

Other sources such as requesting information on group structure, financial statements, voting rights and attestations from accountants or auditors may be useful. Ongoing monitoring of accounts (seeking to understand linkages and financial flows) and checking controllers of accounts (e.g., signatories, those who effect transactions, and those with legal power to sign contractual documents), are other indirect avenues used to reveal the true BOs. Beneficial owners of legal persons and legal arrangements should be identified, and their identities independently verified during on boarding of their customers, on occasional transactions and on an on-going basis.

Institutions should guard against individuals who seek to use other people's fraudulently obtained identification documents for purposes of opening accounts in financial institutions.

Institutions should take note of corporate entities which require licenses from supervisory bodies or Government approval to open accounts. Where a license is required for an entity to conduct a particular business, no institution should open an account for such an entity without obtaining a genuine and copy of a valid license issued by the responsible supervisory authority. Similarly, where the approval of a government body is required before a person opens an account, an institution should ensure that a copy of the Government approval is part of the CDD documents. The necessary verifications should be conducted.

Where CDD information is incomplete, institutions should refuse business relationships, or not perform the transaction. The institution should make a suspicious transaction report and take remediation actions as may be necessary.

For occasional transactions, mostly taking place in the forex bureaus and money or value transfer service (MVTs) providers, National ID or valid passport would suffice in the identification of customers prior to execution of a transaction. But this should not apply to mobile money service providers (MMSP). MMSPs should not apply simplified CDD to all individual customers without any regard to the varying risks posed by them. Risk-based approach requires that institutions assess the risks posed by a customer or category of customers and take measures to mitigate the ML/TF/PF risks. Not all MMSP customers pose the same ML/TF/PF risk. MMSPs should therefore risk-profile their customer in accordance with the law and duly approved risk assessment policies and procedures.

Remote on-boarding poses ML/TF/PF risks. Institutions have a duty to identify customers during remote or virtual on-boarding. Request for photocopies of identification documents is not synonymous with identifying the person. While some institutions have employed biometric verification for remote on-boarding, institutions are advised to devise other affordable methods which enable them to identify customers to be on-boarded virtually or remotely.

Platforms that facilitate virtual on-boarding such as mobile money platforms have been the subject of fraud due to forgery of documents and identity theft. This vulnerability is due to the fact that MMSPs do not identify the customer and verify that the customer who registered the SIM with the service provider, is the same one seeking to access mobile financial services. MMSPs should address this vulnerability as a matter of urgency.

Institutions should collect information that supports source of funds and source of wealth. This information should be effectively verified using any reliable independent source, or institutions should employ any other methods to satisfy themselves as to the authenticity of the documents collected. Systems to verify source of funds and/or wealth should be implemented by all institutions.

Institutions seeking to use a third party should ensure the third party is regulated, supervised or monitored by a competent authority and has measures in place for compliance with customer due diligence and record-keeping requirements in line with international best practice. Where third parties perform some elements of KYC/CDD (as in the case of bank-driven mobile products), institutions retain the prime responsibility for KYC/CDD to mitigate challenges in accessing the KYC/CDD information from the third parties.

Signing agreements that transfer the KYC/CDD responsibilities and liability to the third parties is not supported in law. For institutions using agents, they should always ensure that they identify and verify the beneficial owner (BO) of their agents/third parties. Institutions that elect to use third parties should ensure that they retain and have the right to access CDD information from the third parties.

Institutions should take note that trust deeds do not in all cases disclose the ultimate beneficiaries as understood in AML/CFT law. For example, a corporate entity may be listed as the beneficiary in a trust deed. For AML/CFT/CPF purposes, the corporate entity is not a BO since BOs are natural persons.

3.0 APPLICATION OF EDD MEASURES

An institution should determine, based on its own criteria, whether a particular customer poses a higher risk. Some customers and entities may pose specific risks depending on the nature of the business, the occupation of the customer, or the nature of anticipated transaction activity.

Some factors to consider include:

- Customers conducting their business relationship or transactions in unusual circumstances

- Customers whose structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests.
- Foreign financial institutions, including banks and foreign money service providers such as forex bureaus, and money transmitters.
- Non-bank financial institutions such as money services businesses, casinos and brokers/dealers in securities, and dealers in precious metals, stones, real estate dealers.
- Publicly exposed persons (PEPs).
- Customers from high-risk jurisdictions.
- Resident and Non- resident aliens (NRAs) and accounts held by foreign individuals.
- Foreign corporations and domestic business entities, particularly offshore corporations such as domestic shell companies, private investment companies and international business corporations located in high-risk geographic locations.
- Cash-intensive businesses, including, for example, supermarkets, convenience stores, restaurants, retail stores, liquor stores, wholesale distributors.
- Foreign and domestic non-governmental organizations and charities.
- Professional service providers.
- Any other person identified as high risk in the national risk assessment and sectoral risk assessment.
- Any other person the institution considers high risk

Institutions should ensure on-going monitoring on high-risk customers.

4.0 RECORD KEEPING REQUIREMENTS

Record keeping is a key requirement of POCAMLA and POCAML Regulations. Under Regulation 42 of POCAML Regulations, institutions are required to:

- maintain and keep records of all transaction, both domestic and international, 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.
- keep all records obtained through customer due diligence measures such as copies or records of official documents like passports, identification cards or similar documents, account files and business correspondence including the results of any analysis undertaken such as inquiries to establish the background and purpose of complex, unusual, large transactions for seven years.
- ensure that 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 if any, the amount and date of the instrument, the number if any of the instrument and details of any endorsements appearing on the instrument are retained.
- ensure that all customer due diligence information and transaction records are made available swiftly to domestic competent authorities upon appropriate authority.

It has been observed that some institutions do not keep complete and accurate records on CDD and transactions. Institutions are therefore advised to ensure that complete and accurate records are kept and in a manner that they can easily be retrieved for reference purposes

5.0 PURPOSE OF THE CIRCULAR

The purpose of the Circular is to:

- i) Remind institutions of their obligations on CDD, EDD and record keeping.
- ii) Require institutions to get a good understanding of the amended AML/CFT/CPF laws and apply them accordingly.

Yours faithfully,



GERALD A. NYOMA
DIRECTOR, BANK SUPERVISION

Cc: Dr. Habil Olaka
Chief Executive Officer
Kenya Bankers Association
13th Floor, International Life House
Mama Ngina Street
NAIROBI

Ms. Caroline Karanja
Chief Executive Officer
Association of Microfinance Banks (AMFI)
P.O. Box 1701-00100
NAIROBI

Mr. Saitoti Maika
Director General
Financial Reporting Centre
UAP-Old Mutual Towers
NAIROBI