ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM

CUSTOMER DUE DILIGENCE GUIDELINES

FOR

THE SUPERVISED FINANCIAL INSTITUTIONS

SEPTEMBER 2022

Content

1. Introduction

1.1 The Customer Due Diligence (CDD) Guideline has been prepared in accordance with the requirement of the Section 6 (27) of the Anti-Money Laundering (Amendment) Act 2017 which stipulates that a competent authority *(hereafter referred to as Bank of Uganda or BOU)* shall establish guidelines to assist accountable persons *(hereafter referred to as Supervised Financial Institutions or SFIs)* to implement and comply with the anti-money laundering (AML) and combatting of terrorism (CTF) requirements provided in the AML Act.

1.2 The prudential requirements regarding CDD requirements which SFIs should comply with are prescribed in Principle 29: - Abuse of financial services – (Essential Criteria 5) of the Basel Core Principles for Effective Supervision (September 2012). Additionally, some of the Financial Action Task Force (FATF) 40 Recommendations *(including Rec. 10, 12, 13, 16, 17 and 19)* prescribes the standards for technical compliance with the AML/CFT obligations of SFIs regarding customer due diligence.

1.3 The statutory and legal requirements indicating the objectives of CDD and for SFIs to conduct customer due diligence are prescribed in Section 6 of the Anti-Money Laundering (Amendment) Act, 2017[1] and Part V or regulations 13 – 17 of the AML Regulations, 2015.

1.4 This CDD Guideline is intended to set out appropriate *supervisory* and *prudential practices* relating to the applicable AML/CFT laws and regulations regarding implementation of CDD measures in SFIs. Therefore, SFIs should incorporate and implement the supervisory and prudential aspects of the guideline in their practices as appropriate or as a minimum standard to align their AML/CFT practices regarding compliance with the CDD requirements.

1.5 The requirements of the CDD Guideline should be implemented by all SFIs in in Uganda which includes Commercial Banks (CBs), Credit Institutions (CIs), Micro-finance Deposit Taking Institution (MDIs), Foreign Exchange Bureaus (FXB) and Money Remittances Companies (MRs).

1.6 The CDD supervisory and prudential practices provided in this Guideline sets out the minimum benchmark to enable the SFIs know and understand their customers, business relationships and the ML/TF risks associated with such customers or business relationships. Accordingly, SFIs should institute a framework to implement the CDD requirements and obligations which at a minimum encompasses the following key aspects.

(a) customer acceptance policy that identifies customers and business relationships that the sfi will not accept based on identified risks.

[1] *Please refer to the Anti-Money Laundering (AML) Amendment Act, 2017 which stipulates a replacement of the entire Section 6 of the Principal Act (the AML Act, 2013).*

(b) Customer identification and verification processes which should include;

(i) verifying that any person purporting to act on behalf of the customer is so authorised, and identifying and verifying the identity of that person,

(ii) identification of beneficial ownership, and taking reasonable measures to verify the identity of the beneficial owner (s),

(iii) understanding the purpose and nature of the business relationship, and

(iv) conducting risk-based reviews to ensure that records are updated and relevant.

(c) Policies and processes/procedures to monitor and recognise unusual or potentially suspicious transactions. SFIs should refer to the Suspicious Transaction Reporting (STR) Guidance issued by the Bank of Uganda for more details regarding STR.

(d) Enhanced due diligence (EDD) on politically exposed persons (PEPs), high-risk customers or business relationships including correspondent banking, wire transfers and high-risk countries.

(e) Clear rules on record keeping on customer due diligence documents, individual transactions and their retention period.

(f) Conducting ongoing due diligence programme on the customers and business relationship, including:

(i) scrutinising transactions undertaken throughout the course of the customer activities or business relationship to ensure that the transactions being conducted are consistent with the sfi's knowledge of the customer, their business and risk profile, including where necessary, the source of wealth and funds; and

(ii) ensuring that documents, data or information collected under the customer due diligence process are kept up-to-date and relevant, by undertaking reviews of existing records, particularly for high risk categories of customers or business relationships.

(g) Timing of verification of customer and ultimate beneficial owner identity;

(h) A mechanism for applying CDD measures on existing customers[2];

(i) The management of incomplete CDD measures; and mitigation of the risks of tipping-off during conduct of CDD measures.

[2]*Existing customers refer to customers' existing in the SFIs as at date of the new laws, regulations and guidance notes are brought into force.*

1.7 The CDD Guideline therefore provides a minimum standard for SFIs and is not intended to replace the existing AML/CFT laws and regulations but rather to provide supervisory and prudential clarity on the context of compliance within the framework of the AML/CFT laws, regulations as well as international standards for AML/CFT regarding CDD.

2. Purposes of the customer due diligence Guidelines

2.1 The purpose of the Guideline is to assist SFIs in Uganda in complying with their CDD obligations stipulated in the AML Act, the implementing regulations (the AML Regulations 2015) and the International AML/CFT Standards.

2.2 The customer due diligence Guideline is aimed at ensuring that the SFIs:

(a) identify and verify the identity of a customers or business relationships using reliable, independently sourced documents, data or information.

(b) identify and verify the identity of a person acting on behalf of a customer and the authority to act on behalf of the person or customer.

(c) identify beneficial owners, and to take reasonable measures to verify the identity of beneficial owners and ascertain, in the case of legal persons and arrangements, the ownership and control structure of a customer or business relationship.

(d) obtain information relating to the purpose and nature of the business relationship, and

(e) ensure that any transaction being conducted is consistent with the sfis' knowledge of the customer or business relationship, their nature of business and risk profile, including where necessary, the source of wealth or funds.

3. What is Customer Due Diligence?

3.1 Customer due diligence is the process of collecting a series of information on a prospective customer and as stipulated in Section 6 (2) of the AML (Amendment) Act, 2017 and Regulations 14 of the AML Regulation, 2015 SFIs should undertake CDD under the following circumstances.

(a) before or during the course of opening an account for or establishing a business relationship with a customer.

(b) before carrying out an occasional transaction equal to or above the amount of five thousand currency points *(that is shs.100m)* or its equivalent in foreign currency; whether conducted as a single transaction or several transactions that appear to be linked;

(c) before carrying out an occasional transaction that is a domestic or international wire transfer irrespective of the amount involved;

(d) whenever there is a suspicion of money laundering or terrorism financing;

(e) to understand the ownership and control structure of the customer;

(f) whenever doubts exist about the veracity or adequacy of previously obtained customer identification data;

(g) as may be specified by AML/CFT regulations.

3.2 The customer due diligence processes which should be conducted by the SFIs on a risk sensitive basis on all types of customers or business relationships under the circumstances mentioned in part 3.1 (a) – (f) are prescribed in the AML (Amendment) Act 2017, Section 6 (3) and entails the following measures.

(a) verifying the identity of the client using reliable, independent source documents, data or information.

(b) identifying and taking reasonable measures to verify the identity of a beneficial owner.

(c) understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship to permit the SFI to fulfil its obligations stipulated in the various Acts and Regulations regarding the AML/CFT regime,

(d) if another person is acting on behalf of the customer, identifying and verifying the identity of that other person, and verifying that person's authority to act on behalf of the customer;

(e) taking any other measures as may be advised by the Financial Intelligence Authority.

4. Importance of Customer Due Diligence

4.1 Conducting proper customer due diligence is essential for instituting and maintaining adequate and effective ML/TF preventive measures as well as oversight of the SFI's customers or business relationships and compliance with the SFI's statutory requirement and obligations stipulated in the relevant AML/CFT Acts and regulations.

4.2 Sound customer due diligence procedures have relevance to the safety and soundness of the SFIs, in that:

(a) they help to protect the SFIs' reputation and the integrity of entire banking systems by reducing the likelihood an SFI becoming a vehicle for or a victim of financial crime and suffering the consequential reputational damage.

(b) they constitute an essential part of sound risk management for example by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management.

4.3 The inadequacy or absence of CDD standards can subject the SFI to serious customer and counterparty risks, especially reputational, operational, legal and concentration risks. Any one of them can result in significant financial cost to SFIs as explained below.

(a) *Reputational risk:* The potential that adverse publicity regarding the SFI's business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the SFI. SFIs are especially vulnerable to reputational risk because they can so easily become a vehicle for or a victim of illegal activities perpetrated by their customers. They need to protect themselves by means of continuous vigilance through an effective CDD programme.

(b) *Operational risk:* This is the event of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. Most operational risk in the CDD context relates to weaknesses in the implementation of the CDD measure, ineffective control procedures and failure to practise due diligence.

(c) *Legal risk*: This is the possibility that lawsuits, adverse judgements or contracts that turn out to be unenforceable can disrupt or adversely affect the operations or condition of the SFI. SFIs may become subject to lawsuits resulting from the failure to observe mandatory CDD standards or practices thus consequently resulting to fines and regulatory penalties as well as criminal liabilities and special penalties imposed by supervisors.

(d) *Concentration risk:* This applies on both the assets and liabilities side of the balance sheet.

(i) On the asset side, SFIs are required to have information systems to identify credit concentrations, set limits to restrict exposures to single borrowers or groups of related borrowers. Therefore, without knowing precisely who the customers are, and their relationship with other customers, it will not be possible for the SFI to measure its concentration risk.

(ii) On the liabilities side, concentration risk is closely associated with funding risk, particularly the risk of early and sudden withdrawal of funds by large depositors, with potentially damaging consequences for the SFI's liquidity. Analysing deposit concentrations requires SFIs to understand the characteristics of their depositors, including not only their identities but also the extent to which their actions may be linked with those of other depositors.

5. Risk Based Approach to Customer Due Diligence

5.1 The AML (Amendment) Act, 2017 Section 6 (3) require that SFIs should apply the customer due diligence measures mentioned in Part 3.1 (a) – (f) on a risk sensitive basis/risk-based approach and should take into account the outcome of the customer risk assessment conducted by the SFI. The requirement to conduct risk-based approach for CDD measures is further stipulated in Regulations 15 of the AML Regulations 2015.

5.2 The requirement in 5.1 therefore specifically implies that SFIs should conduct customer or business relationship ML/TF risk rating in order to determine the ML/TF risk level of the customer or business relationship and;

(a) where the ML/TF risk identified by the SFI is high, the SFI should conduct enhanced due diligence measures on the customer or business relationship at each stage of the customer due diligence process and shall continue to be applied on an on-going basis.

(b) where the ML/TF risk identified by the SFI is medium or low, the SFI should have the discretion to conduct simplified due diligence (SDD) measures but this does not apply to cases involving suspicion of ML/TF.

(c) for specific customer types or transactions or business relationships involving politically exposed persons (PEPs), correspondent banking and high-risks countries, SFIs are required to at all times conduct enhanced due diligence measures and continue to be applied on an on-going basis.

5.3 Customer or business relationships ML/TF risk profiling/rating

(a) SFIs should understand the ML/TF risks of its customers, referred to as the customer risk profile or customer risk rating. The program for determining customer risk profiles should be sufficiently detailed to distinguish between significant variations in the ML/TF risks of its customers or business relationships.

(b) Improper identification and assessment of a customer's risk profile can have a cascading effect, creating deficiencies in multiple areas of internal controls and resulting in an overall weakened AML/CFT compliance program.

(c) The assessment of customer risk profile is specific to each SFI and a conclusion regarding the customer risk profile should be based on a consideration of all pertinent customer information. Similar to the SFIs ML/TF risk assessment, there are no required risk profile categories (for example its common to use the three (03) scale approach of; Low, Medium and High) and the number and detail of these categorizations will vary based on the SFI size and complexity.

(d) SFIs should gather sufficient information about the customer risk factors to form an understanding of the nature and purpose of customer relationships at the time of account opening.

(e) The SFI should identify the specific risks of the customer and then conduct an analysis of all pertinent information in order to develop the customer's risk profile. In determining a customer's risk profile, the SFI should consider customer risk factors, such as:

(i) the type of customer relationship:
(ii) products and services used by the customer,
(iii) delivery channels, used by the customer and
(iv) geographic locations of the customer and

The above risks factors should be reviewed on an ongoing basis and the existence of any one single indicator is not necessarily determinative of the existence of a lower or higher customer risks profile.

(f) As with the risk assessment, the SFI may determine that some factors should be weighted more heavily than others. For example, certain products and services used by the customer, the type of customer's business, delivery channels, or the geographic location where the customer does business, may pose a higher risk of ML/TF.

5.4 Description of customer risk factors for determining high and low risk customers

The examples below are not mandatory elements and are included for guidance only and are not intended to be comprehensive. Although they are helpful indicators, they may not be relevant in all circumstances. SFIs should apply the relevant examples indicated below to determine the risk profile of a customer.

(a) High risks customers:

There are circumstances where the risk of ML/TF is high, and enhanced CDD measures have to be taken. When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially higher risk situations may include the following:

(i) ***Customer risk factors:*** Examples include, the business relationship is conducted in unusual circumstances (e.g. significant unexplained geographic distance between the SFI and the customer), non-resident customers, legal persons or arrangements that are personal asset-holding vehicles, companies that have nominee shareholders or shares in bearer form, business that are cash-intensive, the ownership structure of the company appears unusual or excessively complex given the nature of the company's business.

(ii) ***Country or geographic risk factors***: Examples include countries identified by credible sources, such Financial Intelligence Authority, Mutual evaluation or detailed assessment reports or published follow-up reports, as not having adequate AML/CFT systems, countries subject to sanctions, embargos or similar measures issued by, for example, the United Nations, countries identified by credible sources as having significant levels of corruption or other criminal activity, countries or geographic areas identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

(iii) ***Product, service, transaction or delivery channel risk factors:*** Examples include, private banking, anonymous transactions (which may include cash), non-face-to-face business relationships or transaction, payment received from unknown or un-associated third parties.

(b) Low risks customers

There are circumstances where the risk of ML/TF may be low. In such circumstances and provided there has been an adequate analysis of the risk by the SFI consistent with the ML/TF National Risk Assessment, the SFI may apply simplified CDD measures. When assessing the ML/TF risks relating to types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels, examples of potentially lower risk situations include the following:

(i) ***Customer risk factors:*** Examples include, other SFIs where adequate AML/CFT oversight is being undertaken, public companies listed on a stock exchange and subject to disclosure requirementswhich impose requirements to ensure adequate transparency of beneficial ownership, public administrations or enterprises, salary earners, SME entities.

(ii) ***Product, service, transaction or delivery channel risk factors***: Examples include residents using interbank transfers, ATMs, children accounts, elderly accounts, financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes.

(iii) ***Country risk factors:*** Examples include countries identified by credible sources, such as mutual evaluation or detailed assessment reports, as having effective AML/CFT systems and countries identified by credible sources as having a low level of corruption or other criminal activity.

5.5 Customer Information – risk-based procedures

SFIs should take the following attributes into consideration when collecting customer information while following the risk-based procedures for AML/CFT;

(a) The level and type of customer information should be commensurate with the customer's risk profile, therefore the SFI should obtain more customer

information for those customers that have a high customer risk profile and may find that less information for customers with a low customer risk profile is sufficient.

(b) Additionally, the type of appropriate customer information will generally vary depending on the customer risk profile and other factors, for example, whether the customer is a legal entity or an individual. For low risk customers, the SFI may have an inherent understanding of the nature and purpose of the customer relationship (i.e., the customer risk profile) based upon information collected at account opening. As a result, the SFIs may not need to collect any additional customer information for these customers in order to comply with this part of the CDD requirements.

(c) Customers that pose high ML/TF present increased risk exposure to the SFI, therefore the due diligence policies, procedures, and processes should define both when and what additional customer information will be collected based on the customer risk profile and the specific risks posed. Collecting additional information about customers that pose heightened risk, referred to as enhanced due diligence (EDD), is part of an effective due diligence program.

(d) Performing an appropriate level of ongoing due diligence that is commensurate with the customer's risk profile is especially critical in understanding the customer's transactions to assist the SFI in determining when transactions are potentially suspicious. Detailed guidance on Suspicious Transaction Reporting (STR) is provided in the STR Guidelines.

(e) Consistent with the risk-based approach, the SFI should do more in circumstances of high ML/TF risk, as well as to mitigate risks generally. Information provided by higher risk profile customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the SFI. The bank should establish policies and procedures for determining whether and/or when, on the basis of risk, obtaining and reviewing additional customer information, for example through negative media search programs, would be appropriate.

6. Minimum framework for customer due diligence measures

At a minimum, the SFI should develop a customer due diligence (CDD) framework which incorporates the following:

6.1 All the circumstances when the SFIs should conducted customer due diligence which are prescribed in Part 3.1 (a) – (f).

6.2 Customer acceptance policy and procedures:

As a prudential requirement for CDD, SFIs should develop and implement a customer acceptance policy and procedure which should at a minimum include:

(a) A description of the types of customers/business relationships, products and services, distribution channels and geographical areas that are likely or that pose a high risk to the SFIs. In considering the attributes of high risks, SFIs should take into consideration the link with ML/TF predicate offences identified in the ML/TF National Risk Assessment Report provided by the Financial Intelligence Authority (FIA).

(b) A requirement for establishing the country of origin, public or high-profile position, linked accounts, business activities or other risk indicators applicable to the customer.

(c) A tiered CDD process such that Enhanced Due Diligence (EDD) is performed for high-risk customers[3] or business relationships.

(d) A flexible on-boarding process such that the policies do not impede the financial inclusion strategy for Uganda.

(e) Specific recognition of risks of entering or establishing a business relationship or conducting occasional transactions with customers or entities linked to terrorist groups.

(f) SFIs should ensure that the circumstances under which SFIs shall undertake or carry out due diligence measures is established in the procedures manual and effectively communicated to all employees involve in the customer on-boarding process.

(g) SFIs Should comply with Section 6 (4) (a) & (b) of the AMLA (Amendment) Act, 2017 and Regulations 19 – 26 of the AML Regulations, 2015, prescribing the examples of documentation that satisfy customer identification and verification requirements for; natural persons who are citizens or residents, foreign nationals, local entities and other bodies, foreign entities or bodies, beneficiaries of legal persons and arrangements, partnerships, trustees beneficiaries in life insurance related businessand person acting for another.

(h) Consider other obligations such as financial inclusion and data protection provided in the Data Protection and Privacy Act, 2020.

(i) Should involve more than just verifying the identity of a customer, therefore, SFIs should collect and assess all relevant information to ensure that:

(i) It knows its customers, persons purporting[4] to act on behalf of customers and their beneficial owners, where applicable.

---

[3]For example, the policies may require the most basic account-opening requirements for an individual with a small account balance. On the other hand, a quite extensive due diligence would be essential for an individual with a high net worth whose source of funds are unclear.

(ii) Knows what it should expect from doing business with them; and

(iii) Is alert to any potential ML/TF risks arising from the relationship.

(j) Implement the following steps when conducting CDD measures in relation to new and existing customers, products or services.

(i) Where CDD is completed during the establishment of the business relationship, the policies and procedures should specify the defined timeframe in which CDD must be completed. The duration of the defined timeframe should minimise the risk of being unable to contact the customer or return the funds to the original source should there be a requirement to discontinue the business relationship.

(ii) In relation to the circumstances that would result in the discontinuance of a customer or the business relationship and the subsequent effect of such discontinuance, customers should be advised or notified in advance during the on-boarding process; and

(iii) A process that allows the return of funds directly to the source from which they came, where appropriate. SFI should exercise caution when considering the means of doing this, so as not to appear to convert or legitimise such funds.

(iv) Consider whether there is any cause for suspicion of ML/TF in circumstances where CDD is not forthcoming and ensure the STR obligations are fulfilled as required.

(v) Act in the best interest of the customer (or prospective customer), while protecting its integrity by preventing ML/TF, while exhausting all possible avenues before taking any actions that might disadvantage a customer.

6.3 Customer identification and verification due diligence

(a) SFIs should obtain reliable independent source documents for identification and verification of customers. This must be performed under all circumstances which require SFIs to undertake CDD measures stipulated in Section 6 (2) of the AMLA (Amendment) Act, 2017 and Regulation 6 (2) of the AML Regulations 2015.

(b) SFIs should refer to the independent verification of customer identity processes prescribed in the regulations 18 – 27 of the AML Regulations 2015.

---

[4] *Persons acting on behalf of a customer may include power of attorney cases, executor/administrator, vulnerable customers who has a third party acting on their behalf via formal authorization*

(c) SFIs should understand and obtain the most appropriate necessary information on the purpose and intended nature of the customer's business. Depending on the type of customer, the information might include but not limited to the following examples:

(i) information concerning the customer's or beneficial owner's business or occupation/employment.
(ii) information on the types of products or services or distribution channels which the customer intends to use.
(iii) the anticipated level and nature of the activity that is to be undertaken through the business relationship, which may include the number, size and frequency of transactions that are likely to pass through the account.
(iv) any relevant information pertaining to related third parties and their relationships with / to an account for example, beneficiaries; or

(d) For cases of high-risk customers, SFIs should establish the source of funds and wealth of the customer.

(e) While SFIs are required under Section 6 (2) of the AML (Amendment) Act, 2017 and Regulation 6 (2) of the AML Regulations, 2015 to obtain information on the purpose and nature of the business relationship before or during the course of opening an account or establishing a business relationship with a customer, the reliability of this profile should increase over time as the SFI learns more about the customer, their use of products/accounts and the financial activities and services that they require.

(f) Therefore, SFIs should ensure that, any known information on the customer is reviewed and monitor their transactions/activity, to ensure they understand the potentially changing purpose and nature of the business relationship.

6.4 Ongoing monitoring of the customer relationship

(a) On-going monitoring and review of transactions enable the SFI to identify suspicious activity/transactions, eliminate false positives alerts and promptly make Suspicious Transactions Reports/Activities (STRs/SARs) to the FIA and on a risk sensitive basis, maintain and update customer information, including beneficial ownership information of legal entity customers.

(b) Accordingly, at a minimum, the SFI should have in place the following to enable effective on-going monitoring and reviewing of customer transactions or business relationships activities:

(i) The process for identifying, investigating and reporting suspicious transactions or activity (refer to STR Guidelines for further details) to the Financial Intelligence Authority (FIA) should be clearly specified in

the SFI's policies and procedures and communicated to all relevant staff of the SFI through regular training.

(ii) The policies and procedures should contain a clear description of employee's obligations and instructions for the analysis, investigation and reporting of suspicious transaction or activity within the SFI as well as guidance on how to complete such reports.

(iii) The procedures should; reflect the principle of confidentiality; ensure swift investigation; ensure reports contain relevant information and are produced and submitted to the FIA within 48 hours after forming the suspicion.

(iv) The process should ensure that upon submission of a STR/SARs, appropriate action is taken to adequately mitigate the risk of the SFI being used for criminal activities. The actions may include:

- the review of the SFI's risk classification of the customer or account or of the entire business relationship itself.
- the need to escalate the matter to the appropriate level of decision-maker e.g. Obtaining Senior Management or Board approval to determine how to handle the relationship,
- considering any other relevant factors, such as cooperation with FIA.

(c) If the SFI become aware as a result of its ongoing monitoring that customer information, including beneficial ownership information, has materially changed, or the SFI has doubts about the veracity or adequacy of previously obtained customer identification data, it should update the customer information accordingly. Additionally, if this customer information is material and relevant to assessing the risk of a customer relationship, then the SFI should reassess the customer risk profile/rating and follow established policies, procedures, and processes for maintaining or changing the customer risk profile/rating.

(d) The SFI's procedures should establish criteria for when and by whom customer relationships will be reviewed, including updating customer information and reassessing the customer's risk profile. The procedures should indicate who is authorized to change a customer's risk profile. A number of factors may be relevant in determining when it is appropriate to review a customer relationship including, but not limited to:

(i) Significant and unexplained changes in account activity
(ii) Changes in employment or business operation
(iii) Changes in ownership of a business entity
(iv) Red flags identified through suspicious activity monitoring
(v) Results of negative media search programs
(vi) Length of time since customer information was gathered and the customer risk profile assessed

(e) The ongoing monitoring element does not impose a categorical requirement that the SFIs must update customer information on a continuous or periodic basis. However, the SFI should establish policies, procedures, and processes for determining whether and when, on the basis of risk, periodic reviews to update customer information should be conducted to ensure that customer information is current and accurate.

6.5 Standards for relevant and up to date record keeping

SFIs should develop clear standards on record keeping on customer identification and individual/business relationships transactions and their retention period. At a minimum the SFI should ensure;

(a) There is a clear and specific records retention and document retrieval policy and procedures manual which at least stipulate:

(i) the process of relevant CDD document retrieval,
(ii) Access control to document archival centre,
(iii) The acceptable manner in which records are to be kept including by way of original documents as hard copies,

(b) Computer disk or in any other electronic form, continuity/swift availability (within 48 hours of request) of required once requested by the relevant law enforcement authorities.

(c) Proper record keeping which permit the monitoring of relationship with the customers or business transaction, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution.

(d) The customer identification papers and retained copies and all financial transaction records both domestic and international, records obtained through CDD measures, account files, business correspondences and results of any analysis undertaken by the SFI are kept for at least ten (10) years after an account is closed and after the transaction has taken place.

(e) The transaction records kept by the SFIs should at a minimum include the customer identification documents, date, amounts and types of currency involved in the transaction and should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity."

(f) The record keeping policy and procedure should comply with the guidelines or directives regarding record keeping including backup and recovery procedures established by the bank or any other regulations or guidance.

6.6 Customer screening process.

SFIs should perform targeted financial sanctions screening for all new customers before commencing the customer on-boarding process. Accordingly, SFIs should have systems in place to detect prohibited transactions and ensure that;

(a) Customers are screened against United Nation Security Council Resolutions Sanctions (UNSCR) 1267 and 1373 listing at on-boarding for new customers and for existing customers.

(b) Relevant searches are performed at on-boarding and during the course of a customer or business relationship using the customer's name, to determine if a potential customer is known to be of high risk to the SFI e.g. PEPs, designated criminals, terrorist, sanctioned individual/entity, reported in media to be involved in any activity that is adverse in nature.

(c) Before establishing a business, relationship or carrying out an occasional transaction with new customers, the customer should be screened against lists of known or suspected terrorists issued by competent (national and international) authorities.

(d) The ongoing monitoring should verify that existing customers are not entered into these same lists. Therefore, SFIs should institute systems in place to detect and prohibited transactions with existing customers and should also up to date the sanctions list from which their customer data bases are screened immediately when there is change in the listing.

(e) Sanctions screening is not a risk-sensitive due diligence measure and should be carried out irrespective of the risk profile attributed to the customer. For the purpose of terrorist screening, SFIs should adopt automatic screening systems, but it should ensure that such systems are fit for the purpose. SFIs should freeze without delay and without prior notice the funds or other assets of designated persons and entities, following applicable AML/CFT laws and regulations.

(f) SFIs should ensure that a wire transfer to or from a person or entity designated by the United Nations Security Council under any United Nations Security Council Resolution relating to the CFT is prohibited. Accordingly, the SFI should freeze any wire transfer, transaction or account relating to a designated person or entity and immediately notify the Financial Intelligence Authority of any action or attempted action, taken in respect of a prohibited transaction or account.

7. Types of Customer due diligence measures

7.1 Enhanced customer due diligence (EDD)

(a) Enhanced due diligence (EDD) measures shall be applied for all high-risk customers and business relations. Additionally, EDD should be always

applied for specific cases including, politically exposed persons (PEPs), correspondent banking relationships and high-risks countries customers and transactions. The specific EDD measures for these categories of customers are prescribed in Part 8 of this guidance notes.

(b) Other additional cases which should require EDD includes;

(i) all customer or business relationships which the SFI has identified as high risk for ML/TF including non-profit organisations, money remittance companies and foreign exchange bureaus. The attributes for high-risk categories of customers or business relationship have been described in part 5.4 (a).

(ii) beneficiaries of bancassurance products for customers identified as high-risk person or entities.

(iii) persons or customers from, or transactions involving, those countries prescribe, by notice in the Uganda Gazette or FIA website or Bank of Uganda circulars or FATF, as high-risk countries in respect of ML/TF measures.

(c) SFIs should examine, as far as reasonably possible, the background and purpose of all complex, unusual large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose. Where the risks of ML/TF are high, the SFI should conduct EDD measures, consistent with the risks identified.

(d) The SFIs should also increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

(e) In addition to the customer due diligence measures mentioned in part 3.2 (a) – (e) of the guideline, the enhanced CDD measures that could be applied for high-risk business relationships include:

(i) obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.

(ii) obtaining additional information on the intended nature of the business relationship.

(iii) obtaining information on the source of funds or source of wealth of the customer.

(iv) obtaining information on the reasons for intended or performed transactions.

(v) obtaining the approval of senior management to commence or continue the business relationship.

(vi) conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

(vii) requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

7.2 Simplified due diligence (SDD)

7.2.1 SDD is the lowest level of due diligence that can be completed on a customer or business relationship and should be reserved for those instances where the customer type; product/services; and geographical areas risks categorisation combination falls into the **low-risk category** where there is little opportunity or risk of ML/TF. SSD should not be seen as an "automatic exercise", but rather more case-by-case as there may be high risk factors other than those listed in this guideline.

7.2.2 SFIs should at all times conduct adequate analysis of risk before deciding to apply SDD. Additionally, SFIs should be awaree that the ML/TF risks could evolve/change from the time of on boarding a customer. Having a lower ML/TF risk for identification and verification purposes does not automatically mean that the same customer is lower risk for all types of CDD measures, for ongoing monitoring of transactions.

7.2.3 SDD measures which SFIs may apply, include but are not limited to:

(a) Adjusting the timing of CDD where the product or transaction sought has features that limit the use for ML/TF purposes, for example by:

(i) verifying the customer's or beneficial owner's identity after establishment of the business relationship. For example, setting defined thresholds or reasonable time limits, above or after which the identity of the customers or beneficial owners must be verified.

(ii) In the circumstances mention in 7.2.3 (a) (i), the SFIs should make sure that: the process does not result in an exemption from CDD. Systems or processes either manual or automated should be put in place to detect when the threshold or time limit has been reached; and they do not defer CDD or delay obtaining relevant information about the customer.

(b) Adjusting the quality or source of information obtained for identification, verification or monitoring purposes, for example by:

(i) **Self-certification** or accepting information obtained from the customer rather than an independent source when verifying the

beneficial owner's identity. The relevant documents for identification of customers are mentioned in regulations 19 (2) of the AML Regulations 2015.

(ii) Relying on the source of funds to meet some of the CDD requirements, where the risk associated with all aspects of the relationship is very low, for example where the funds are state benefit payments, salary accounts.

(iii) Adjusting the frequency of CDD updates and reviews of the business relationship.

(iv) Adjusting the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only.

(v) SFIs that choose to monitor above a certain threshold only should ensure that the threshold is **set at a reasonable level** and that they have systems in place to identify linked transactions that, together, would exceed that threshold.

7.2.4 When applying SDD measures, SFIs should obtain sufficient information on the risk factors to enable them to be reasonably satisfied that their assessment of the ML/TF risk associated with the relationship is low and is justified.

7.2.5 SFIs should obtain sufficient information about the nature of the business relationship to enable identification of any unusual or suspicious transactions and should note that SDD does not exempt reporting suspicious transactions to the FIA.

7.2.6 If, however at any point during the relationship with the customer, additional information becomes available to the SFI which suggests that the customer or product may pose a higher risk than originally assessed, enhanced due diligence should be conducted.

8. Establishing or conducting specific customer due diligence measures

(a) SFIs should refer to the regulatory requirements specified in Regulations 21 – 26 of the AML Regulations of 2015 regarding **establishing** and **verifying** the identity of;

(i) Local entities and other bodies
(ii) Foreign entities or bodies
(iii) Partnerships
(iv) Trustees
(v) beneficiaries in a legal person or legal arrangement, that is the natural persons exercising control and ownership of a legal person or legal arrangement other than a trust

(vi) beneficiaries in life insurance related businesswhen conduction customer due diligence measures for legal persons and legal arrangement.

(b) SFIs should collect the following information when performing the function of establishing and verifying the identity of the legal person or legal arrangements.

(i) Name, legal form and proof of existence – verification could be obtained, for example, through a certificate of incorporation, a certificate of good standing, a partnership agreement, a deed of trust, or other documentation from a reliable independent source proving the name, form and current existence of the customer.

(ii) The powers that regulate and bind the legal person or arrangement (e.g. the memorandum and articles of association of a company), as well as the names of the relevant persons having a senior management position in the legal person or arrangement (e.g. senior managing directors in a company, trustee(s) of a trust).

(iii) The address of the registered office, and, if different, a principal place of business.

9. Specific steps to identify and verify identity of beneficial owners

9.1. *Legal persons*

(a) In addition to the CDD process in 8 (b) (i) – (iii), when on boarding legal persons SFIs should focus on the identification and verification of the natural person(s) who ultimately owns or controls a customer and / or the natural person on whose behalf a transaction is being conducted.

(b) Accordingly, SFIs should undertake the following when assessing the ultimate ownership and control of the legal person;

(i) controlling ownership of the legal person: the SFIs should identify and verify the identity of the natural person (s) who owns at least five percent (5%) or more shareholding of the legal person.

(ii) Ultimate control of the legal person: the SFIs should consider the ability of the natural person to take relevant decisions and to impose those decisions within the legal person. These natural persons include the shareholder(s), partners(s), board of directors, executive officer(s); settlor(s), trustee(s), beneficiary (ies), nominees, business associates, and close family members.

(c) SFIs should at a minimum undertake the following 3-step approach (referred to as "the cascade") or methodology for determining the beneficial owner(s) of the legal person.

(i) identify the natural person(s) (if any) who ultimately has a controlling ownership interest in a legal person/entity. These are natural persons, holding at least 5% of shareholding in the legal person.

(ii) to the extent that there is doubt under 9.1 (c) (i) above, as to whether the person(s) with the controlling ownership interest is the beneficial owner(s) or where no natural person exerts control through controlling ownership interests, the identity of the natural person(s) (if any) exercising control of the legal person through other means;

(iii) If no natural person is identified in steps 9.1 (c) (i) and (ii) above, the natural person(s) who holds the position of Senior Management Official should be identified.

(d) Where the customer or the owner of the controlling interest is a company listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means) which impose requirements to ensure adequate transparency of beneficial ownership or is a majority-owned subsidiary of such a company, it is not necessaryfor the SFI to identify and verify the identity of any of the shareholders or beneficial owners of that company.

9.2 *Legal Arrangements*

(a) In addition to the CDD process in 8 (b) (i) – (iii), when on boarding legal arrangement SFIs should focus on the identification and verification of the natural person(s) or the beneficiaries on whose behalf a transaction is being conducted.

(b) For trust, the SFI should establish and verify the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other natural person exercisingultimate effective control over the trust (including through a chain of control/ownership).

(c) For other types of legal arrangements, the SFI should establish and verify the identity of thepersons in equivalent or similar positions mentioned in 9.2 (b).

9.3 *PoliticallyExposed persons (PEPs)*

9.3.1 In accordance with the FATF Recommendation 12 criterion 12.1 (a), Section 6 (7) of the AML (Amendment) Act, of 2017, Regulations 29 (1) of the AML Regulations 2015, SFIs should implement appropriate risk management systems to determine whether a person or customer is a politically exposed person (PEP) namely, a domestic, foreign, or international PEP.

9.3.2 As defined in the AML (Amendment) Act of 2017, PEPs mean an individual who is or has been entrusted with a prominent public function in Uganda or another country, and includes:

(a) A Head of State or Head of Government,
(b) Senior politician,
(c) Senior Government Official,
(d) Judicial or Military official,
(e) Senior Executive of a State-owned corporation,
(f) Important party officials.
(g) A person who is or has been entrusted with a prominent function by an international organization, including a member of senior management, director, deputy director or member of a board and includes a related person of the individual.
(h) SFIs should also institute mechanism for the PEP to disclose his/her close family members and close associatesor appropriate mechanism to determine the close family member and close associate a of a PEPs and include them within the control framework established for PEPs.

9.3.3 The close family member(s) of a PEP shall include the PEP's spouse, their children and their spouses (if any), parents and the siblings of the PEP, uncles, aunty, sister-in-law and brother-in-law while close associate include the PEP's widely and publicly known close business colleagues or personal advisors, in particular persons acting in a financial fiduciary capacity.

9.3.4 In relation to the PEP definition in 9.3.2 above, SFIs should focus on establishing whether the person or the beneficial owner(s) holding the prominent public function or important positions, with substantial authority over policy, operations or the use or allocation of government-owned resources have more influence which would pose greater ML/TF risks for the SFI and should accordingly be categorised as a PEPfor the purposes of control and oversight frameworks.

9.3.5 SFIs should consider a range of factors when determining whether a particular holder of a prominent public function has the requisite seniority, prominence or importance to be categorised as a PEP. The relevant factors could include:

(a) Assessing the nature of the relevant PEP and the PEP's vulnerability to corruption as per various publicly available, independent indices,
(b) The official responsibilities of the PEP
(c) The nature of the PEP (honorary or salaried PEP),
(d) The level of authority of the PEP over governmental activities and over other officials,
(e) Whether the function affords the PEP access to significant government assets and funds or the ability to direct the awards of government tenders or contracts and
(f) Whether the PEP has links to an industry that is particularly prone to corruption.

9.3.6 In establishing the appropriate risk management framework for identification of PEPs, SFIs should obtain or develop a PEP list, and depending on the size of the SFIs and geographical footprint, an SFI may choose to source its PEP data for

screening purposes from a third-party vendor or some SFIs may choose to develop their own internal database.

9.3.7 In relation to the implementation of appropriate risk management systems to determine whether a customer or beneficial owner of an entity is a PEP, SFIs should perform at a minimum the following processes:

(a) The account opening documents should solicit for voluntary disclosure by a customer or business relationship whether the customer or the beneficial owner is a PEP or the business relationship involves a PEPs. Additionally, once a customer has voluntarily declared PEP status, the account opening forms should solicit for voluntary disclosure of close family member (s) or close associates.

(b) Develop a process which regularly collects PEPs information and updates the PEPs data base using information; published in the gazette by the Electoral Commission of Uganda, of Senior Political Party Officials in Uganda, list of information on Heads of Government Ministries, Departments and Agencies, Judicial Service Commissions, Ministry of Defence and other publicly available credible information.

(c) Develop processes which regularly collect PEPs information and updates the PEPs data base on foreign PEPs using publicly available and credible sources of information on person who is or has been entrusted with a prominent function by an international organization.

(d) Regularly undertake processes to identify PEPs who may already be existing in their customer data base or business relationships and immediately update the identified PEP on-boarding documents by performing the procedures required for PEPs.

(e) Establish appropriate guidelines to monitor business relationships for domestic PEPs where the ML/TF risk is high.

9.3.8 The involvement of a PEP in the management of an entity-based relationship, increases the risks involved in establishing or maintaining an account or a business relationship with such an entity, but may not necessitate the categorisation of the entity as a PEP. However, accounts for trusts, personal investment companies, foundations, operating companies or other entity-based accounts should, if established for the specific benefit of a PEP or the PEP close family member or close associate, should be subjected by the SFI to the control framework appropriate for PEPs.

9.3.9 SFIs should implement a framework which enables identification of beneficiaries in life insurance related business in compliance with the statutory requirement in regulations 26 (2) of the AML Regulations 2015. Accordingly, SFIs should:

(a) take reasonable measures to determine whether a person or customer or the beneficiary of the life insurance policy is a PEP and the identification should be done before the proceeds are paid.

(b) The Officer/Staff of the SFI must inform the responsible member of Senior management before the pay-out of the policy proceeds, conduct enhanced scrutiny on the whole business relationship with the policyholder, and consider making a suspicious transaction report where applicable.

9.3.10 *Foreign Politically Exposed Persons*

(a) In addition to the customer due diligence requirements in part 3.2, SFIs should undertake the following measures for identified foreign politically Exposed persons.

(i) Obtain senior management approval for establishing (or continuing, for existing customers) such business relationships. Senior Management approval included approvals froma member of the Senior management (Officers vetted by Bank of Uganda) with direct reporting to Managing Director or Executive Director or by the Executive Director/Managing Director.

(ii) obtain information on the close family members or close associates.

(iii) determine the purpose of the transaction or account and the expected volume and nature of account activity.

(iv) review publicly available sources of information on the PEP and

(v) conduct enhanced on-going monitoring of the business relationship, once the account has been established. The period of conducting ongoing monitoring of the PEP should be stipulated in the documented PEP procedural manual.

(vi) take adequate measures to establish the source of wealth and funds of the customer or beneficial owner in the business relationship or transaction.

9.3.11 *Domestic and International Politically Exposed Persons*

(a) In addition to the customer due diligence requirements, SFIs should undertake the following measures for identified domestic and International politically exposed persons.

(i) The SFIs should conduct customer risk assessment/rating to determine whether the domestic or international PEP is high risk for ML/TF.

(ii) If the domestic or international PEP is deemded high risk for ML/TF, then in accordance with the AML (Amendement) Act, 2017 Section 6 (7) (c), the SFIs should undertake all the measures listed in part 9.3.10 (a) (i) – (vi).

(iii) For domestic and international PEPs with low ML/TF risk profile, the SFI should undertake measures mentioned in part 9.3.10 (a) (i) – (v) only

9.3.12 Regarding the various aspects of PEP enhance due diligence of undertaking reasonable measures to establish the source of wealth and funds, enhance ongoing monitoring, approval of senior management, SFIs should perform the following processes:

(a) When undertaking reasonable measures to establish the source of wealth and funds:

(i) assess the activities that have generated the total net worth of the PEP (that is, the activities that produced the PEP's funds and property);

(ii) evaluate the origin and the means of transfer for funds that are involved in the transaction (for example, their occupation, business activities, proceeds of sale, corporate dividends)

(b) When applying enhanced ongoing monitoring of the business relationship:

(i) regularly review the information held on the PEP and their beneficial owners (where relevant) to ensure that any new or emerging information that could affect the risk assessment is identified in a timely manner.

(ii) The frequency of ongoing monitoring should be determined by the SFI commensurate with the high risk associated with the PEP relationship.

(c) Obtaining approval of senior management before establishing or continuing a business relationship with a PEP;

(i) By establishing appropriate policies and procedures clearly setting out; the reporting and escalation of PEP relationships to Senior Management; the timelines for obtaining Senior Management sign-off; and the level of seniority required to approve a PEP relationship.

(ii) Allocating responsibility for the approval of PEP relationships and ensure that the approval of a PEP relationship is conducted by Officers who are appropriately skilled and empowered, and this process is subject to appropriate oversight.

(iii) Determining the level of seniority for sign-off by the level of increased ML/TF risk associated with the PEP business relationship. The Senior

Manager approving a PEP business relationship should have sufficient seniority and oversight to take informed decisions on issues that directly impact the SFI's ML/TF risk profile.

(iv) taking into consideration, the level of ML/TF risk that the SFI would be exposed to if it entered into that business relationship with the PEP; and what resources the SFI would require to mitigate the risk effectively.

(v) ensuring that, the matter on whether to enter, or to continue to carry on a business relationship with a PEP, is discussed at Senior management level and reported to the Board of Directors, the corresponding ML/TF risks are acknowledged; and the decision reached is documented.

(vi) where a review of the information and documentation provided by a PEP during ongoing review reveals ML/TF concerns the matter on whether to continue to carry on a business relationship with a PEP, is discussed at Senior management level and reported to the Board of Directors and the decision reached is documented.

(vii) however, where a PEP has been reviewed and there are no ML/TF risks concerns, sign off by a Senior Managing Official is sufficient. However, the Board should be regularly informed (at least quarterly) about the numbers of existing PEPs in the SFI.

9.3.13 SFIs should verify the ownership and management structures of the correspondent financial institution including determining whether a PEP has ownership or control of the correspondent financial institution.

(a) If the SFI identify a PEP, the SFI should perform the guidance regarding foreign domestic or international PEPs describe in this guidance.

9.3.14 Generally, SFI should at a minimum implement the following key components of PEP risks management.

(a) *Identification – New Customers:* SFIs should have risk-based procedures to determine whether a customer is a PEP, before the relationship is established. Once a new customer is determined to be a PEP, the SFI should risk assess the customer and apply appropriate due diligence measures in a timely manner.

(b) *Identification – Existing Customers:* where an SFI becomes aware that an individual has become a PEP it should apply risk based due diligence and controls.

(c) *Customer Risk Assessment:* Once it has been determined that a new or existing customer is a PEP, the SFI should undertake a risk assessment to determine both the level of financial crime risk posed by PEP and the

proportionate levels of due diligence and monitoring that are required. The SFI should use its customer risk assessment process, taking into account risk factors such as geography, product, business type and delivery channel. For geographic risk, the SFI should consider information available from reliable and independent sources as to the levels of systemic corruption in the country of political exposure.

(d) *Due Diligence:* Once the PEP has been subject to risk assessment, SFIs should apply risk based due diligence procedures, which should include:

(i) Understanding and documenting the length of time, the title or position and country in which the PEP holds, or held, political exposure. If the individual customer is a close family member or close associate, the relationship of the person to the PEP must be documented.

(ii) Understanding and documenting the nature and intended purpose of the relationship/account, the source of the initial funds (where appropriate) and the anticipated levels of account activity.

(iii) Understanding and documenting the PEP's source of funds and source of wealth (e.g. salary and compensation from official duties and wealth derived from other sources). Where the financial crime risks are high or there are doubts as to the veracity of the information provided by the PEP, the SFIs should validate this information using independent and reliable sources. SFIs may use internet and media searches to determine and/or validate this information, having considered the potential limitations of such sources

(iv) Conduct Negative News/Adverse Media screening on the PEP and evaluate any positive hits.

(v) When the due diligence on an immediate family member or close associate of a PEP indicates that the source of funds originates from the PEP, then the SFI should determine and document the PEP's sources of funds and wealth. Negative News/Adverse Media Screening on the PEP who funds the account may assist in establishing whether the PEP has deliberately attempted to disguise their involvement in funding the account.

(e) *Approval:* PEP relationships should be approved by senior management who understand both the financial crime risk and their responsibility within the SFI's AML control environment. The level of seniority should be directly proportionate to the nature of the SFI and the money laundering risk posed by the PEP.

(f) *Enhanced Monitoring (manual or automated):* accounts with a PEP relationship should, using an RBA, be subject to proportionate enhanced monitoring to detect unusual and potentially suspicious activity.

(g) *Periodic reviews for existing PEP customers:* such relationships should be subject to periodic review to ensure that due diligence information remains current, and the risk assessment and associated controls remain appropriate. Frequency of periodic reviews should be determined by the risk of the customer and be documented appropriately. If the risk of the PEP has materially changed since the last review/approval (Death/Divorce), the SFI may consider subjecting the PEP to re-approval by relevant senior management.

(h) *PEP Risk Exposure (SFI/Portfolio wide):* Beyond the individual customer reviews an SFI should review its overall exposure to PEP risk, in particular on a business line level, with senior management confirming that the risk exposure remains within the SFI's defined risk appetite.

(i) *Training & Education:* The business are the first line of defence in preventing and detecting financial crime and also have a crucial role to play in identifying customers or potential customers who are PEPs. It is therefore vital that the risk, policies, procedures and processes associated with PEPs are communicated to relevant employees and their managers and form part of the regular AML training programme.

9.3.15 PEP Declassification

(a) Although PEP influence may substantially reduce as soon as they have left office, a PEP may have been able to acquire his or her wealth illicitly, so that a high level of scrutiny regarding such individuals may be warranted even after they have left office. Continuation of maintaining a PEP status should be consistent with a Risk Based Approach (RBA) managing the PEP. Certain higher risk PEPs may warrant maintaining classification as a PEP indefinitely, while for other categories SFIs should undertake holistic approach to assess whether the PEP should be de-classified.

(b) When SFIs consider de-classification of a PEP, the following considerations should be made when determining the length of time appropriate post departure of a PEP.

(i) The PEP position held and its susceptibility to corruption or misappropriation of state funds or assets;
(ii) The length of time in office and likelihood of return to office in future;
(iii) The level of transparency about the source of wealth and origin of funds, in particular those funds generated as a consequence of office held • Links to any industries that are high risk for corruption;
(iv) The level of transactions processed through the account
(v) Whether there is relevant adverse information about the PEP widely published in reputable sources
(vi) Politicalconnection of the PEP that remains once they have left office.

(c) Where the PEP is deceased but was the source of funds/wealth for close family members' or close associates', a risk-based assessment will need to be made to determine whether those relationships still merit appropriate levels of EDD on their own merits or whether they should be declassified.

(d) Any declassification of a PEP should be subject to Senior management review and approval, the review should be documented, and their prior PEP status should be noted in the event of a suspicious activity reporting about the declassified PEP.

9.4 *Enhanced Due Diligence in relations to Correspondent Banking*

(a) In accordance with the requirements stipulated in Regulations 31 of the AML Regulations 2015, SFIs who are correspondent or respondent entities should perform risk assessments of the relationships before on-boarding the relationship.

(b) The risk assessment of the correspondent or respondent relationship should considera number of risk factors including but not limited to:

(i) The jurisdiction in which the correspondent or respondent institution is incorporated in and the AML / CFT regulatory regime as well as quality of the supervisor oversight of the correspondent or respondent institution is subject to.

(ii) The ownership and management structure of the correspondent or respondent institution, including any role performed by or influenced by beneficial owners or PEPs.

(iii) The business purpose of the relationship.

(iv) Operations and transaction volumes.

(v) The correspondent or respondent institution's customer base.

(vi) The quality of the correspondent or respondent institution's AML/CFT systems and controls, and

(vii) Any negative information known about the correspondent or respondent institution or its affiliates.

(viii) obtain approval from senior management before establishing new correspondent or respondentrelationships; The Senior Management approval process should in principle adhere with the governance standards as stipulated in the PEPs approval process.

(ix) obtain written approval from the Central Bank before establishing a new correspondent financial institution relationship.

(c) The conclusion of the risk assessment in describe in 9.4 (b) (i) – (vii) above should determine the appropriate risk rating attached to a particular correspondent or respondent institution and drive the level of enhanced due diligence (EDD) applied and the frequency of relationship review.

(d) SFIs who are correspondent institutions should regularly screen respondent institutions, their controllers, beneficial owners and any other connected persons, to identify for PEP connections or persons, or affiliated or subsidiary entities subject to financial sanctions.

(e) SFIs shall institute a process which prohibits entering or continuing with, a correspondent banking relationship with a shell bank, or a respondent institution that is known to permit its accounts to be used by a shell bank.

(f) SFIs should regularly review and identify correspondent banking relationships with high-risk countries in respect of ML/TF, whenever information on high-risk countries in respect of ML/TF has been published by the FIA. SFI should amend and if necessary, termination correspondent or respondent banking relationships with high-risk countries.

(g) SFIs should with immediate effect apply the requirements regarding correspondent banking or respondent banking relationships established prior to 2013.

(h) SFIs who are correspondent institutions should ensure that sufficient information is obtained on all respondent relationships and particularly for any respondent relationship where EDD is applied (or respondent SFIs from high-risk jurisdictions/countries as published by the FIA).

(i) SFIs who are correspondent institutions should perform periodic reviews of higher risk correspondent or respondent relationships at least on an annual basis. The following trigger events at a minimum should be considered by the SFI:

(i) Material changes in ownership and/or management structure.
(ii) Re-classification of the jurisdiction where the respondent institution is located.
(iii) Identification of a PEP relationship.
(iv) Identification of adverse media on the respondent institution.

9.5 *Enhanced Due Diligence in relation to High-risk Countries*

(a) In accordance with the requirements stipulated in Regulations 44 of the AML Regulations 2015, SFIs should institute effective internal control processes or systems which enable timely update of the information on high-risk countries.

(b) SFIs should access information on high-risk countries from; the FATF website in March and June of every calendar year, the FIA website or notice

in the Uganda Gazette and through the BOU circulars regarding list of high risks countries.

(c) Customer or business relationships or transactions from the identified high-risk countries must be subjected to specific elements of Enhanced Customer Due Diligence (EDD) process such as:

(i) Obtaining additional information on thepurpose of transactions and nature of the business relationship. This information may include:

- The number, size and frequency of transactions that are likely to pass through the account, to enable the SFI to spot deviations that might give rise to suspicion.
- The destination of funds.
- The nature of the customer's or beneficial owner's business, to enable the SFI better understand the likely nature of the business relationship.

(ii) Obtaining senior management approval to continue the relationship. The Senior Management approval process should in principle adhere with the governance standards as stipulated in the PEPs approval process.

(iii) Enhanced monitoring of transactions.

(iv) reviewing, amending and if necessary, terminating of correspondent banking relationships.

(v) Obtaining addition information customer or beneficial owner's identity or ownership and control structure. This information may include assessing any adverse media information, family members and close business associates and past and present business activities of the entity.

(vi) the source of funds or wealth of the customer: The source of funds or source of wealth may be verified, inter alia, by reference to VAT and income tax returns, copies of audited accounts, pay slips, property registration or independent media reports.

9.6 *Client accounts opened by professional intermediaries*

(a) SFI should put in place internal control process to identify customers or business relationships which relates to Law firms/entities or a professional intermediary who open accounts on behalf of a single client. In such circumstances the SFIs should identify and verify the identity of the person, entity or client on who behalf the account is being opened.

(b) SFIs often hold "pooled" accounts managed by professional intermediaries on behalf of entities such as mutual funds, pension funds, money funds,

lawyers or stockbrokers, electronic money balances held by trustees linked to licensed electronic money providers, that represent funds held on deposit or in escrow for a range of clients. Where funds held by the intermediary are not co-mingled at the SFI, but where there are "sub-accounts" which can be attributable to each beneficial owner, all beneficial owners of the account held by the intermediary must be identified and verified on a risk-based approach.

(c) SFIs should accept such accounts only on the condition that they are able to establish that the intermediary has engaged in a sound customer due diligence process and has the systems and controls to allocate the assets in the pooled accounts to the relevant beneficiaries.

(d) Where the intermediary is not empowered to furnish the required information on beneficiaries to the SFI, for example, lawyersbound by professional secrecy codes or when that intermediary is not subject to due diligence standards or to the requirements of comprehensive anti-money laundering legislation, then the SFI should not permit the intermediary to open an account.

9.7 *Non-face-to-face customers*

(a) SFIs are increasing opening accounts on behalf of customers who do not present themselves for in-personal interview especially for non-resident customers on account of innovations in electronic banking.

(b) SFIs should apply effective customer identification procedures and on-going monitoring standards for non-face-to-face customers as for those customers who avail themselves for interview.

(c) For electronic banking, SFIs should institute specific and adequate measures to mitigate the higher risk by:

(i) Certification of documents presented.

(ii) Requisition of additional documents to complement those which are required for face-to-face customers.

(iii) Independent contact with the customer by the SFI.
(iv) Third-party introduction, for example by an introducer subject to the following criteria.

- The SFIs should have carefully assess whether the introducers are "fit and proper" and exercised the necessary due diligence in accordance with the SFIs policies and procedures.

- It must comply with the minimum customer due diligence practices in the SFIs policies and procedures.

- the customer due diligence procedures of the introducer should be as rigorous as those which the SFI would have conducted itself for the customer.

- the SFI must satisfy itself as to the reliability of the systems put in place by the introducer to verify the identity of the customer.

- the SFI must reach agreement with the introducer that it will be permitted to verify the due diligence undertaken by the introducer at any stage.

- all relevant identification data and other documentation pertaining to the customer's identity should be immediately submitted by the introducer to the SFI, who must carefully review the documentation provided. Such information must be available for review by Bank of Uganda and Financial Intelligence Authority.

- Conductperiodic reviews to ensure that an introducer which it relies on continues to conform to the criteria set out above.

(d) SFIs should proactively assess various risks posed by the new or emerging technologies and design customer identification procedures with due regard to such risks.

9.8 *Private Banking Product*

(a) SFIs that offer private banking services are particularly exposed to reputational risk andshould therefore apply Enhanced Due Diligence (EDD) to such operations.

(b) Private banking accounts, which by nature involve a large measure of confidentiality, can be opened in the name of an individual, a commercial business, a trust, an intermediary or a personalised investment company.

(c) All new clients and new accounts should be approved by at least one person of appropriate seniority, other than the private banking relationship manager.

(d) If particular safeguards are put in place internally to protect confidentiality of private banking customers and their business, banks must still ensure that at least equivalent scrutiny and monitoring of these customers and their business can be conducted, e.g. they must be open to review by compliance officers and auditors.

9.9 *Wire Transfer Customer due diligence*

(a) SFIs undertaking a wire transfer shall ensure that all information accompanying the domestic or cross-border wire transfer includes:

(i) complete originator information such as the name, address, account number of the originator and other related information.

(ii) the national identification number, or passport number or date and place of birth of the originator, where applicable.

(iii) the complete beneficiary information, such as the name of the beneficiary, address of the beneficiary, the account number of the beneficiary, the Society for Worldwide International Financial Telecommunication (SWIFT) code and other information, and the information shall remain with the fund transfer or related message through the payment chain.; and

(iv) the beneficiary account number, where such an account is used to process the transaction, and in the absence of an account number, the unique transaction reference number shall be included.

(b) SFIs should ensure that an intermediary institution in the payment chain provides originator and beneficiary information that accompanies an electronic funds transfer.

(c) SFIs shall monitor and report to the Financial Intelligence Authority electronic funds transfers which do not contain complete originator and beneficiary information.

(d) SFIs should restrict or terminate a business relationship with customers or entities that persistently fails to include complete originator and beneficiary information in its electronic funds transfer.

9.10 *Money or Value Transfer Service (MVTS)*

(a) SFIs should ensure compliance with all of the relevant requirements of part 8.10, directly or through their agents.

(b) In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider should be required to:

(i) take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and

(ii) file an STR in any country affected by the suspicious wire transfer and make relevant transaction information available to the Financial Intelligence Authority.

9.11 *Reliance on third parties*

(a) In accordance with the AML (amendments) Act 2017, SFIs may rely on third parties to perform elements of the customer due diligence measures set out in this guideline as well as AML/CFT laws and regulations or to introduce business. However, where the SFI relies on third parties, the ultimate responsibility for CDD measures remains with the SFI.

(b) The conditions should be satisfied for the SFI to rely on third parties are as follows:

(i) The SFIs should immediately obtain all the necessary information concerning elements the CDD measures as prescribed in the guidelines, AML/CFT laws and regulations.

(ii) The SFI should establish an internal policy and procedural manual or process to ensure that identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

(iii) The SFI should obtained adequate documentation which demonstrates that the third party is regulated, supervised or monitored for, and has measures in place to comply with, CDD measures and recordkeeping requirements.

(c) When a SFI relies on a third party that is part of the same financial group, and

(i) that group applies CDD and record-keeping requirements, in line with guidelines or applicable AML/CFT laws and regulations in Uganda, and

(ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a Supervisory Authority;

then the SFI may apply measures under 9.9 (a) (ii) & (iii) through its group programme.

10. Mechanism for applying customer due diligence on "existing customer"[5];

10.1 SFIs should apply CDD requirements to *existing customers*based on materiality and risk and conduct due diligence on such existing relationships at appropriate times, taking into account whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

10.2 To ensure that records remain up-to-date and relevant, SFIs should undertake regular reviews of existing records on a risk based approached. Appropriate

[5] "Existing customers" refers to customers' existing in the SFIs as at date of the new laws, regulations and guidance notes are brought into force.

time to do so is when a transaction of significance takes place, whencustomer documentation standards change substantially, or when there is a material change in the way the customer's account is operated.

10.3 However, if a SFI becomes aware at any time that it lacks sufficient information about an existing customer, it should take steps to ensure that all relevant information is obtained as quickly as possible.

11. Approaches to the management of incomplete CDD measures

11.1 Where a SFI is unable to complete the relevant CDD measures within the SFI's stipulated period of time:

(a) it should notcommence business relations or perform the transaction.
(b) terminate the business relationship; and
(c) consider making a suspicious transaction report (STR) in relation to the customer.

12. Mitigating the Risk of tipping-off during conduct of CDD measures

In cases where a SFI has formed a suspicion of money laundering or terrorist financing, and the SFI reasonably believe that performing the CDD process will tip-off the customer, the SFI shall not pursue the CDD process, and instead file an Suspicious Activity Report (SAR) to the Financial Intelligence Authority.

13. Training and awareness

13.1 The Section 6 (17) (d) stipulate the significance of SFIs developing and implementing programs for the prevention of ML/TF that are appropriate to the risks and the size of the SFI's business and the programs shall include training an employee training program to ensure that employees, managers and directors are kept informed of all the aspects of the AML/CFT requirements concerning due diligence measures.

13.2 Therefore, SFIs should implement ongoing employee training programmes so that the employees, managers and directors are adequately trained to implement the bank's AML/CFT policies, procedures and the CDD guidelines.

13.3 SFI should take steps to ensure that staffs understand bank wide ML/TF risk assessment, and how it affects their daily work; the bank's CDD policies, procedures and this guideline and how they have to be applied.

13.4 The SFI should implement CDD training in a manner that the timing and content of the training should be adopted or relevant to the SFIs and its business needs or risk profile, tailored to staff functions and specific jobs responsibilities and length of service with the SFI to ensure that the employee has sufficient knowledge and information to effectively implement the SFIs AML/CFT policies and procedures.

13.5 SFIs should regularly update the CDD training program depending on the national or sectoral merging e ML/TF threats and vulnerabilities as well as typologies.

13.6 SFIs should at least annually conduct refresher training to ensure that staff are reminded of their obligations and their knowledge and expertise are kept up to date. However, for avoidance of doubt, the scope and frequency of such training should be tailored to the risk factors to which employees are exposed due to their responsibilities and the level and nature of risk present in the SFIs.

14. Review of the Guideline

SFIs should ensure full compliance with this customer due diligence guidelines. Additionally, while implementing the requirements of this guidelines, the SFIs are requested to compile and record any comments or relating questions for clarification regarding the implementation of these guidelines. The comments should be forwarded to:

The Office of the Executive Director,
Supervision Directorate,
Bank of Uganda

Sources of Information

1. *Methodology for assessing technical compliance with the FATF recommendations and the effectiveness of AML/CFT systems: (fatf-gafi.org)*

2. *International standards on combating money laundering and the financing of terrorism & proliferation the FATF recommendations:(fatf-gafi.org)*

3. *Wolfsberg Frequently Asked Questions ("FAQ's") on (wolfsberg-principles.com) (The Wolfsberg Group, Wolfsberg Guidance on Politically Exposed Persons;*

4. *Basel Committee on Banking Supervision Guidelines Sound management of risks related to money laundering and financing of terrorism.*

5. *Anti-Money Laundering (AML) Act 2003, AML (Amendment) Act 2017, AML Regulations 2015, AML Regulations Amendment Act 2022*