مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.

RESTRICTED: Not to be disclosed outside the Financial Institutions until Public

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

GUIDANCE FOR LICENSED FINANCIAL INSTITUTIONS ON CUSTOMER DUE DILIGENCE/KNOW YOUR CUSTOMER AND RECORD-KEEPING

November 30, 2024

Contents

1. Introduction

Conducting customer due diligence ("CDD") and implementing know your customer ("KYC") and record-keeping controls are foundational parts of compliance with anti-money laundering, combating the financing of terrorism, and counter proliferation financing ("AML/CFT/CPF"), sanctions, counter-fraud, and anti-bribery and corruption laws. Specifically, adequate CDD/KYC is the cornerstone for licensed financial institution ("LFI") when establishing an understanding of customers, including a customer's business practices and expected activity for which to detect suspicious activity in the future. According to both the United Arab Emirates ("UAE")'s laws and regulations in addition to financial crimes compliance ("FCC") global standards, all LFIs must have a written CDD/KYC program reasonably designed to mitigate financial crime risks specific to their institution.

It is critical for LFIs to have robust record-keeping requirements and controls to enable an LFI to comply swiftly with information requests from Competent Authorities. These records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) and the identification of the persons involved so as to provide information to a requesting authority, conduct lookbacks to identify and remediate compliance gaps, among other measures as necessary. Complete records of customers and transactions should be secure, yet easily accessible, to enable an LFI to work with authorities, regulators and outside consultants in cases where the LFI or its regulator has identified areas needed improvement or remediation.

As such, LFIs should understand the importance of CDD/KYC and the elements that comprise a robust CDD/KYC and record-keeping framework, which should be tailored to the size, complexity, and risk profile of the LFI and the specific characteristics of the LFI's customer base.

1.1. Purpose

Article 44.13 of the *Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") LFIs and registered hawala providers ("RHPs") of their statutory obligations under the legal and regulatory framework in force in the UAE, as detailed in section 1.3 below. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 3090/2021 dated 29/06/2021) (hereinafter CBUAE's *AML/CFT Guidelines for Financial Institutions)* and any amendments or updates thereof.[1] As such, while this

[1] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, circulars, and notices, and outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF")[2] and industry best practices. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs and RHPs should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs and RHPs expected to demonstrate compliance with its requirements within one month from its coming into effect.

1.2. Applicability

Unless otherwise noted, this Guidance applies to all natural and legal persons, which are Financial Institutions or Licensees, or any other defined term which brings all entities within the scope of licensed and/or supervised entities by the CBUAE, in the following categories:

- National banks, branches of foreign banks, exchange houses, finance companies, investment companies, payment service providers, virtual asset service providers ("VASPs"), payment token service providers, registered hawala providers;
- Insurance companies, agencies, and brokers; and
- Other covered financial institutions not specified above, or any other entities that are licensed or registered by the CBUAE and are engaged in financial activities that fall under AML/CFT/CPF regulations.

For LFI's with operations outside the UAE, this guidance applies to their UAE-based activities and should inform group-wide standards, while adhering to applicable regulations in the local jurisdiction.

The term "Licensed Financial Institutions (LFIs)" covers all entities listed in this section (i.e., Section 1.2. – Applicability).

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

[2] For example, please see: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

- Federal Decree-Law No. (14) of 2018, Regarding the Central Bank & Organization of Financial Institutions and Activities, and its amendments ("CBUAE Law").
- Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and its amendments ("AML-CFT Law");
- Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations ("AML-CFT Decision") and its amendments;
- Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council ("UNSC") Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74"), and its amendments;
- Guidance for Licensed Financial Institutions on Digital Identification for Customer Due Diligence;
- Cabinet Decision No. (58) of 2020 regulating the Beneficial Owner Procedures ("Cabinet Decision 58"); and
- CBUAE/BSD Notice No. 1943.2022 Regarding AML/CFT Minimum Standards and Supervisory Expectations.

1.4. Acronyms

Terms	Description
AML	Anti-money laundering
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer due diligence
CFT	Combating the financing of terrorism
EDD	Enhanced due diligence
Executive Office	Executive Office for Control and Non-Proliferation
FATF	Financial Action Task Force
LFI	Licensed financial institution
FIU	Financial Intelligence Unit
KYC	Know your customer
LFI	Licensed financial institution
ML	Money laundering
PEP	Politically exposed person
RHP	Registered hawala providers

SAR	Suspicious activity report
SDD	Simplified due diligence
SoF	Source of funds
SoW	Source of wealth
SAR	Suspicious activity report
STR	Suspicious transaction report
TF	Terrorist financing
TFS	Targeted financial sanctions
UN	United Nations
UNSC	United Nations Security Council
UNSCR	UN Security Council Resolution

2. The Role and Significance of CDD/KYC and Recordkeeping

2.1. The Significance of CDD and KYC

The financial sector continues to grow in complexity. The traditional model of a local customer physically opening an account and utilizing products and services at a local LFI is increasingly being replaced by global customer base engaging in large volumes of cross-border transactions. The growing use of online banking allows customers to establish a relationship without ever coming in direct face-to-face contact with an LFI's employees, posing challenges to an LFI's effort to verify the identity of a customer. Adding to these transparency challenges, customers are able to utilize the services of different non-bank and third-party payment processors, potentially in jurisdictions where the customer does not physically reside, as internet- and smartphone-based payment applications are involved in a growing percentage of payment transactions across the globe. In addition, the interconnected elements of the international financial system and global nature of trade, with numerous participants, serve as a justification for a high volume of cross-border payments, often originated electronically and processed straight through without an LFI's intervention or oversight.

Overall, the significance of CDD/KYC is highlighted by the following factors:

- **Sophisticated financial crimes threats:** Criminals are using more sophisticated means to engage in money laundering and other financial crimes, while remaining undetected, by hiding behind complex corporate structures or creating false identities through fake documentation, whether by stealing a real person's identity or by combining real and fake information to create a new identity. Such practices are disruptive and result in significant financial losses for countries, LFIs, and other market participants. Appropriately identifying and verifying customers, including

understanding the nature of a customer's business, helps LFIs protect their institution against financial crime.

- **Non-compliance risks**: Regulatory, reputational, and financial consequences of non-compliance are all serious repercussions resulting from ineffective CDD/KYC controls. Without appropriate CDD/KYC to mitigate against financial crime, an LFI risks money laundering and other financial crime incidents that put an LFI's reputation on the line and can can cause financial harm to LFIs in a number of ways. The occurrence of such incidents also associates the LFI in the minds of the public with financial crime. This hurts an LFI through a loss of confidence in the LFI's ability to uphold its commitment to financial integrity.
- **Interconnected financial system**: The UAE's financial system is increasingly interconnected, and the harm done by illicit actors engaging in financial crime is global, impacting the financial integrity and stability of the international financial system as a whole. Appropriate CDD/KYC controls not only ensures the financial integrity of the UAE's financial system overall, but it also helps LFIs build and maintain trusting relationships with correspondent banks. In the context of correspondent banking specifically, LFIs are expected to conduct sufficient CDD/KYC on customers having direct access to the account of a correspondent bank.

All of this requires an LFI to remain vigilant when designing, employing, adjusting, and testing their risk-based CDD/KYC program to ensure that the LFI has an adequate understanding of their customers' identities and expected transactions.

Both "CDD" and "KYC" terms are used interchangeably in this Guidance to refer to an LFI's overall process of verifying the identity of its customers and assessing the risk of engaging these customers, both prior to onboarding and throughout the customer relationship. CDD/KYC is an ongoing, risk-based process to collect, record, and assess relevant information about customers and the customer's related parties, business profile, and transactions to appropriately assign and monitor the ML/TF/PF and other financial crimes risks of the customer. CDD/KYC often happens before a new customer is onboarded, and then at regular intervals throughout a customer's relationship with the LFI. Specifically, LFIs should perform CDD/KYC in the following scenarios:

- **When establishing a business relationship:** Ahead of establishing a new customer-business relationship and conducting any transactions on a customer's behalf, LFIs should perform due diligence to verify the identity of the customer and its related parties, evaluate the customer's risk profile, understand the customer's business and expected transactions, and ensure the customer is not using a fake identity to access the LFI's products and services.
- **To analyse occasional transactions:** Certain transactions might require further CDD/KYC measures. For example, transactions over a certain monetary amount will require an LFI to review and potentially update a customer's CDD/KYC information.
- **When there is suspicious activity:** LFIs should implement additional CDD/KYC checks if the customer engages in unusual or potentially suspicious activity that requires further investigation, either due to the presence of a red flag or because the customer is engaging in activity that is

inconsistent with their historical profile established at onboarding, or if the customer has been classified as a Related Party to a party of concern identified through transactional review, ownership and control, or public domain. Ultimately if the LFI has reasonable grounds to suspect that a transaction, attempted transaction, or funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime, the LFI is required to file a Suspicious Transaction Report ("STR") or Suspicious Activity Report ("SAR") with the UAE's Financial Intelligence Unit ("FIU").

- **Unreliable identification:** If information a customer has provided is inaccurate, incomplete, or does not meet an LFI's internal requirements for CDD/KYC, LFIs should implement additional CDD/KYC measures to ensure that they can properly establish the identity of the customer and the nature and purpose of the customer's relationship with the LFI.
- **Periodic and trigger-event reviews:** LFIs should implement periodic CDD/KYC reviews for all existing customers with the review frequency corresponding to the risk profile of a customer, as well as one-off reviews due to a particular trigger event occurring related to the customer.

There are four core elements of a CDD/KYC program, each addressed in a further detail below in section 3 *Customer Due Diligence*:

- Identifying a customer and verifying the customer's identity;
- Identifying beneficial owner(s) and key senior personnel of a legal entity customer and verifying their identity;
- Understanding the nature and purpose of a customer relationship to develop a customer risk profile; and
- Ongoing monitoring of customer activity for reporting suspicious transactions and updating customer information and risk profile, as necessary.

2.2. The Importance of Record-keeping

Record-keeping is an essential element of designing and implementing an LFI's internal control framework, and a robust record-keeping program involves the entire LFI. From front-line employees to senior management, all employees should be aware of their LFI's record-keeping policies and understand the importance of storing data in a safe and reliable manner to support any internal processes, as well as regulatory requests and law enforcement inquiries.

Specifically, accurate and up-to-date records enable an LFI's internal stakeholders, regulators, and law enforcement to reconstruct and analyse information and patterns of activity, including the amounts and types of currency involved, if any, as part of any money laundering or terrorist financing investigations.

While there is no definitive set of record-keeping requirements for every customer type, there should be enough documentation that underpins an LFI's onboarding, periodic, and event-driven CDD/KYC review process to demonstrate:

- Why a specific customer was onboarded;
- How the customer was risk rated, and
- What steps the LFI took to monitor the customer's activity to ensure it corresponded to the customer's risk profile throughout the business relationship with the LFI.

In addition, should a customer's activity rise to a level of a reportable suspicious activity or transaction, LFIs are expected to be able to produce detailed, well-organized supporting documentation if law enforcement has any follow-up inquiries about the customer and activity in question.

As such, adequate record-keeping ensures that all information, including documents and records provided by customers, is preserved in a manner that will allow easy access, when needed, available at all times for inspection as authorized by UAE laws and regulations. Additional detail regarding record-keeping can be found in section 4.

3. Customer Due Diligence

3.1. General Principles

A customer can be anyone who performs a one-off or occasional financial activity or transaction or anyone who establishes an ongoing commercial or financial relationship with the LFI. LFIs should develop and implement appropriate, risk-based, and sufficiently detailed procedures for collecting identifying information and conducting CDD/KYC both at onboarding and on a periodic basis thereafter. These procedures should address, at a minimum:

- Obtaining, analysing, and storing pre-defined types of information about a customer, whether a natural or legal person, its beneficial owners and related parties, the nature of their business, source of wealth, and other data points for purposes of developing a customer risk profile;
- Verifying collected information via documentary or non-documentary means or a combination of both, on a risk-sensitive basis;
- Assigning the customer a risk profile and adjusting it over time;
- Conducting enhanced due diligence ("EDD") on customers that have been deemed higher risk;
- Refreshing customer information periodically or due to certain incident triggers that are formally documented and defined by the LFI; and
- Conducting ongoing transactions monitoring to verify that a customer's activity is in line with their stated or historic activity and customer profile overall, to update customer information when necessary, and to be able to identify and report suspicious transactions.

In addition to conducting CDD/KYC before or during onboarding and periodically thereafter, LFIs should undertake CDD measures in the following cases:

- Carrying out occasional transactions in favour of a customer for amounts equal to or exceeding AED 55,000, whether the transaction is carried out in a single transaction or in several transactions that appear to be linked;
- Carrying out occasional transactions in the form of wire transfers for amounts equal to or exceeding AED 3,500;
- Where there is a suspicion of crime; or
- Where there are doubts about the veracity or adequacy of previously obtained customer identification data.

Best Practices to Ensure Consistent Application of CDD/KYC

It is advisable that LFIs with a presence and operations in multiple countries develop standardized, global CDD/KYC procedures to ensure uniform collection, verification, and record-keeping of customer data across all offices, branches, and majority-owned subsidiaries. A global approach to CDD/KYC enables an LFI to have a comprehensive view of its customer base, standardize its risk ratings, and apply uniform controls and analytic tools across different products and jurisdictions.

In the case of where the AML/CFT laws and regulations of an LFI's host country (outside of the UAE) are less stringent than those of UAE, LFIs should ensure that foreign branches and majority-owned subsidiaries in these countries implement the CDD/KYC requirements of the UAE, to the extent permitted under a host country's AML/CFT laws and regulations. This is important as deficient CDD/KYC measures undertaken by an LFI's subsidiary in another country may limit the overall effectiveness of the LFI's AML/CFT controls at the group level.

In addition, it is further recommended that LFIs develop detailed, standardized customer on-boarding forms, with the information gathered ultimately forming part of a customer's CDD record. Such forms can be tailored to specific customer types (for example, individuals; trusts; operating companies; publicly listed companies; correspondent banks; investment companies). The selection of these customer types also may be due to the customer's risk, such as if the customer type is known to be higher risk from an FCC perspective and requires specific documents to be collected as part of the LFI's EDD process, or if the customer is lower-risk and requires Simplified Due Diligence ("SDD") as discussed in section 3.5 *Simplified Due Diligence for Lower-Risk Scenarios*. LFIs may also seek to streamline their onboarding process and tailor their onboarding forms to those customer types that are most prevalent to their institution (for example, the LFI onboards a high number of insurance companies which represents a significant portion of the LFI's customer base).

LFIs can also choose to develop two types of on-boarding forms, (i) a customer facing form, and (ii) an internal on-boarding form, with the latter being used for additional data gathering, data verification, and analysis performed by the LFI's staff.

It is important to remind staff that CDD/KYC should not be treated as a "check-the-box" exercise. Staff should critically assess information provided by a customer, seek additional information or clarifications, if necessary, and raise any identified issues to the UAE FIU. Typically, it is the first line of defence and front-line (i.e., customer facing) employees who are the most equipped to identify red flags when it comes to CDD/KYC—including by assessing a customer's behaviour at onboarding, reviewing customer documentation for authenticity, and determining whether there are any challenges associated with obtaining a customer's CDD/KYC information. Whenever possible, LFIs should incorporate a "four-eye" principle into their CDD/KYC procedures with regard to the verification of customer identification documentation and other CDD/KYC information, including inputting the relevant data into their information technology systems.

Since CDD/KYC is a risk-driven process, as part of CDD/KYC procedures, LFIs should also prescribe situations where a customer should undergo either EDD or SDD. EDD is warranted in situations where a customer typically presents higher financial crime risk, such as relationships with foreign PEPs, relationships with persons from high-risk countries, and correspondent banking and other similar relationships. LFI's CDD/KYC procedures should prescribe what additional information the LFI should collect as part of EDD. For further detail on EDD, please refer to section 3.6 *Enhanced Due Diligence for Higher-Risk Scenarios*. SDD can be applied in customer relationships that do not raise red flags and that involve UAE government entities, publicly listed companies, or customers rated as low risk under the LFI's documented customer risk assessment methodology. For further detail on SDD, please refer to section 3.5 *Simplified Due Diligence for Lower-Risk Scenarios*.

LFIs should not establish or maintain relationships with customers who are unable or unwilling to provide required CDD/KYC information, whether at onboarding or as a part of ongoing monitoring, periodic review, or event-driven review processes. Where required CDD/KYC processes cannot be completed, including where the customer refuses to provide CDD/KYC information; the customer provides apparently false or misleading information or documentation; the customer is suspected of engaging in identity theft; or the customer provides information that differs from information obtained during the verification process or subsequent ongoing monitoring; the matter must be escalated through an LFI's appropriate channels to be considered for suspicious activity and transaction reporting. Where discrepancies cannot be resolved, the account should be rejected or restricted and closed in a commercially reasonable manner, taking into consideration the legal requirements applicable to the LFI maintaining the customer relationship.[3]

The LFI which does not comply with the section 3 in the guidance:

- Shall not open the account, commence business relations or perform the transaction; and
- Shall file a Suspicious Transaction Report (STR) with the UAE FIU.

[3] For example, positive balances on the account(s) or long-term loans and other types of relationships may also present challenges if an LFI decided to offboard a customer for compliance considerations. In such instances, the LFI may consider imposing sufficient restrictions on customer's account(s) to ensure the customer does not commit financial crimes and work towards reducing the balance to zero.

In case, the LFI has already commenced the business relationship, it shall terminate the business relationship and submit a Suspicious Transaction Report.

3.2. Customer and Beneficial Owner Identification and Verification

Under Article 8 of the AML-CFT Decision, LFIs are required to identify and verify the identities of all customers, regardless of whether they are establishing a permanent relationship or require a one-off service (such as exchanging currencies or transferring funds to a walk-in customer). The identification and verification requirements also apply equally to natural and legal persons or legal arrangements. Verification of a customer's identity should be performed using documents, data, or information from a reliable and independent source. Examples of reliable and independent sources include official government-issued documents (e.g., passport, license), documents that are certified by a third party (e.g., a notary), and documents issued from a reputable third party or public authority (e.g., utility bills, stock exchange disclosure reports, credit reporting agencies, etc.).

Customer identification and verification allows an LFI to form a reasonable ground that it knows the true identity of the customer. An LFI can use documentary or non-documentary methods of identification and verification, or a combination of both, which is further discussed in section 3.2.4 *Documentary and Non-Documentary Means of Customer Identification and Verification*. The LFI's CDD/KYC procedures should describe these methods in an easy-to-understand manner, including explaining the types of documents an LFI finds acceptable for CDD/KYC. Customers should generally be identified and verified prior to establishing a business relationship. However, in exceptional circumstances, as per Article 4.3 of the AML-CFT Decision, where there is no ML/TF/PF suspicion and a customer's ML/TF/PF risks are assessed to be low, an LFI may complete the verification of the customer's identity after establishing a business relationship, as set forth in section 3.5 *Simplified Due Diligence for Lower-Risk Scenarios*. Additional detail regarding customer identification and verification can be found in the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 6.3.1.[4]

3.2.1. *Natural Persons*

Under Article 8.1 of the AML-CFT Decision for natural persons, LFIs should verify an individual's identity using the following markers:

- Person's name (as identified on an identification card or travel document, and taking a copy of and attaching the copy of the original and valid identification card or travel document);
- Nationality;
- Address (i.e., the permanent residential address);
- Date and place of birth;

[4] Available at https://www.centralbank.ae/media/zhqjanp0/cbuae-guidelines-on-aml-cft-for-fis-june-2021_1.pdf

- Name and address of employer;
- For minors, documentation to verify the identity and relationship status of parent and/or legal guardian;The intended purpose and nature of the business relationship (obtaining, when necessary, information related to this purpose); and
- PEP status, determining whether the customer or beneficial owner is a PEP.[5]

3.2.2. *Legal Persons and Arrangements*

Under Article 8.1 of the AML-CFT Decision, for legal persons or legal arrangements, LFIs should verify the legal person or arrangement using the following markers:

- The name, legal form, and memorandum of association;
- Headquarters office address or the principal place of business. (If the legal person or arrangement is a foreigner, it must mention the name and address of its legal representative in the UAE and submit the necessary documents as proof);
- Articles of association or any similar documents, attested by the competent authority within the UAE;
- Key countries of operations, if any outside of the UAE;
- Names of relevant persons holding senior management positions with the legal person or legal arrangement (i.e., a Chief Executive Officer, a Chief Financial Officer, a Chief Operating Officer, a General Partner, a Treasurer, a President or persons with similar authority), and all account signatories or persons otherwise authorized to give instructions on the account(s);
- Information on the ownership and structure of the legal entity, up to an individual level of ownership in accordance with section 3.2.5 *Beneficial Ownership Identification and Verification*;
- The intended purpose and nature of the business relationship (obtaining, when necessary, information related to the purpose of the customer's business relationship with the LFI); and
- The nature of the customer's business.

Depending on its risk assessment, an LFI may develop and implement additional methods of customer identification and verification tied to certain types of customers or financial products. For example, for an individual customer that is onboarding via an online application, an LFI may consider collecting additional information such as a phone number, email address, and/or tax identification number; for a corporate customer that meets a certain risk threshold, an LFI may choose to conduct a site visit. This information may confirm the location of a customer and also serve as an additional verification method should a customer later claim loss of access to the account.

[5] LFIs should obtain approval from senior management if the customer or beneficial owner is a foreign PEP or there are high-risk markers associated with the domestic PEP or head of international organization.

For all relevant individuals associated with (e.g., ultimate beneficial owners ("UBOs") a legal person and persons acting on behalf of the customer), the LFI should verify their identity using the same markers as when verifying individual customer's identity in accordance with section 3.2.1 *Natural Persons*.

3.2.3. *Natural Persons Acting on Behalf of the Customer*

LFIs are required to verify that any person purporting to act on behalf of the customer is authorized, and LFIs should verify the identity of that person as described above. Persons acting on behalf of customers can range from, for example, lawyers collecting or disbursing funds through their customer's trust accounts to a broker authorized to execute trading orders on a customer's securities account. In these instances, LFIs should seek to obtain documentation establishing the individual's authority to act on behalf of the customer.

Examples of acceptable evidence to establish the individual's authority to act on behalf of the customer include copies of board resolutions, articles of incorporation, other constitutional documents or extracts from company registries, a Letter of Authority, or Power of Attorney. A representative's authority may be implicit if the individual is a director or equivalent officer for a legal person customer, provided the LFI's first line employee has no cause to believe the director is a nominee shareholder acting on behalf of another individual.

3.2.4. *Documentary and Non-Documentary Means of Customer Identification and Verification*

Under Article 8 of the AML-CFT Decision, LFIs are required to identify each customer and verify the customer's identity using documents, data, or any other identification information from **a reliable and independent source**. This requirement is technology neutral and expressly permits LFIs to use documentary as well as non-documentary sources (i.e., information or data) when performing identification and verification. An LFI's CDD/KYC procedures should describe the process and authorized means of verifying a customer's identity, including scenarios, if any, where more than one verification method should be used.

Documentary sources mean that an LFI can use pre-defined types of documents to verify a customer's identity, such as an unexpired government-issued registrations, documentation, or certifications, or documentation issued by other respectable third parties, such as another LFI or public authority.

In the case of verifying an individual, the following are examples of documentary methods (all documents should be valid, unaltered, and unexpired):

- To confirm an individual's identity, an LFI can use an official government-issued identification document, such as a passport, national identification card, so long as the document bears a photograph of the individual. The use of these documents extends to confirming an individual's nationality and national ID number;

- To confirm the date and place of birth, an LFI can use a birth certificate, a passport, or a national identification card; and
- To confirm residency address, an LFI can ask for a recent (e.g., such as within the last three months) utility bill, correspondence from a UAE government office, tenancy contract, tax statement, a deed for purchase of a residence, or a mortgage statement.

In the case of verifying a legal entity, the following are examples of documentary methods:

- Certificate of incorporation bearing an official government agency seal;
- An official extract from a government-maintained corporate registry; or
- An official government-issued corporate ID;

Considering the wide usage of counterfeit and fraudulent documents, an LFI may consider in certain cases such as onboarding of a non-resident customer, to review more than a single document to ensure it can form a reasonable belief that it knows the true identity of the customer. In addition, LFIs should take steps to understand those types of identification documents that are legally valid in the relevant jurisdictions of a non-resident customer. If an LFI is unfamiliar with the type of document issued by a foreign government authority, it can ask the customer to provide a notarized or apostilled copy of the document or a copy certified by an embassy official.

Non-documentary sources refer to a range of verification methods other than a government-issued document. For example, for both individual and legal entity customers, it may include:

- Scheduling a face-to-face meeting with a customer;
- Contacting a customer via phone, mail, or email to confirm they are still valid;
- Checking references with other financial institutions;
- Independently verifying the customer's identity or registration, beneficial ownership, and confirming current active status via public or private databases, corporate registries, or a credit bureau; or
- Visiting the legal person customer's place of business, if practical.

An LFI should consider utilizing non-documentary sources as part of the enhanced due diligence measures undertaken for high-risk scenarios such as: the LFI being unfamiliar with a document presented, the LFI opening the account remotely or via mobile/online application without the customer or its authorized representatives physically present at the LFI, or if an LFI's front-line employees identify red flags during the customer onboarding process.

3.2.4.1. Digital Identification and Verification

Separately from using documentary and non-documentary methods to verify a customer's identity, financial institutions around the world and in the UAE are increasingly relying on digital methods for customer identification and verification. With the rapid development of digital systems and solutions, more and more

financial institutions offer customers the ability to be onboarded remotely, without ever visiting a financial institution's office or branches. Some financial institutions also operate on a fully online basis, without establishing physical locations. Even further, many government authorities, including in the UAE, are moving towards adopting full or partial digital system solutions for issuing, verifying, recording, and securely maintaining individual IDs or corporate registries or certificates.

Thus, it is important for LFIs to develop procedures that are responsive to these new technological advances, but at the same time, consider unique risks that they may represent and ensure that digital identification and verification processes are adequate and appropriate.

Recognizing these developments, Article 8 of the AML-CFT Decision does not impose any restrictions on the form—physical or digital—that identity evidence must take, nor does it impose limitations as to the use of digital identification systems for the purpose of linking a customer's verified identity to a unique, real-life individual, provided this is done using a "reliable" and "independent" source. Digital identification systems use electronic (as opposed to physical) means to assert and prove a person's identity, including through the use of:

- Electronic databases to obtain, confirm, store, and/or manage identity evidence;
- Digital credentials to authenticate identity for accessing mobile, online, and offline applications;
- Biometrics to help identify and/or authenticate individuals; and
- Digital application program interfaces, platforms, and protocols that facilitate online identification and the verification and authentication of identity.

As such, LFIs are permitted to utilize digital identification systems as well as physical forms to perform customer identification and verification, consistent with the expectations set forth in this Guidance and the CBUAE's *Guidance for LFIs on Digital Identification for Customer Due Diligence*.[6] Thus, although digital means of identification are separate and distinct from the documentary or non-documentary means, the governing principle remains the same – an LFI should not establish a customer relationship or offer services to a person unless the LFI forms a reasonable belief that it knows the true identity of the customer.

In the digital identification context, the requirement that digital source documents, data, or information must be "reliable" and "independent" means that the digital identification system used to conduct CDD/KYC relies upon technology, adequate governance, processes, and procedures that provide an appropriate level of confidence that the system produces accurate results. Reliability and independence in this sense depends specifically on the effective application of mitigating measures to prevent and manage risks related to **identity proofing and enrollment**, such as the risks of an applicant using falsified identity evidence or another individual's identity, as well as risks related to **authentication and identity lifecycle management**, including various risks that bad actors will illicitly obtain an individual's legitimate identity credentials and use them to open an account or obtain unauthorized access to products, services, and data.

[6] Available at https://www.centralbank.ae/media/nphlwxs5/guidance-for-lfis-on-digital-identification-for-customer-due-diligence.pdf

See the CBUAE's *Guidance for LFIs on Digital Identification for Customer Due Diligence*, section 4 for additional information regarding the risks and corresponding mitigating measures related to the use of digital identification systems for specified CDD/KYC purposes.

Overall, LFIs should be aware of and utilize the following national-level identification systems and processes that exist or are under development in the UAE:

- **Emirates ID**, the mandatory identity card for all UAE citizens and residents issued by the Federal Authority for Identity, Citizenship, Customs and Ports Security ("CIP"). While issued as a physical card, the Emirates ID uses public key infrastructure to attach individual identities to digital certificates that be used to sign and encrypt data, as well as fingerprint biometrics. LFIs should use the online Validation Gateway maintained by the CIP[7] when verifying an Emirates ID card and should keep a copy of the card and evidence of its digital verification in accordance with its record-keeping policies.
- **UAE Pass**,[8] the UAE's first national digital identity and signature solution that enables users – citizens, residents, and visitors in the UAE – to identify themselves to government service providers in all emirates through a smartphone-based authentication protocol and to sign documents digitally with a high level of security. The UAE Pass app uses biometric facial recognition software to verify and register users without requiring an in-person visit to a government services centre.
- **Emirates Facial Recognition**, an initiative launched by the UAE Ministry of Interior and CIP, together with private sector partners. The facial recognition initiative includes a "face fingerprint" system for digital verification of digital transactions and remote identities.

3.2.5. *Beneficial Ownership Identification and Verification*

The AML-CFT Law defines a beneficial owner as a "natural person who owns or exercises effective ultimate control, directly or indirectly, over a customer or the natural person on whose behalf a transaction is being conducted or, the natural person who exercises effective ultimate control over a legal person or Legal Arrangement, whether directly or through a chain of ownership, control or other indirect means."

Accordingly, under Article 9 of the AML-CFT Decision, LFIs are required to identify the UBOs of the customer and take measures to verify the identity of such persons using information, data, or statistics acquired from a reliable source, as follows:

- For any **legal person customer:**
    - The identities of all beneficial owners of such customer are defined as all individuals who, individually or jointly, have a controlling ownership interest in the legal person of 25 percent or more.

[7] Available at https://icp.gov.ae/en/icp-validation-gateway/
[8] For more information, see https://uaepass.ae/

- Where no individual meets this description (for example, in case of publicly listed entities), the LFI is required to identify and verify the identity of the individual(s) holding the senior management position in the entity. This option should be used only as a last resort, however, and when the LFI is confident that no one individual, or small group of individuals, exercises control over the customer.

- For any **legal arrangement customer**:
  - The identity of the settlor, the trustee(s), or anyone holding a similar position, the beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control over the legal arrangement.
  - LFIs should also obtain sufficient information regarding the beneficial owner to enable verification of his/her identity at the time of payment or at the time he/she intends to exercise his/her legally acquired rights.

The UBO of a legal person or arrangement must be an individual. With one exception listed below, another legal person cannot be classified as the UBO of a customer, no matter what percentage it owns. LFIs should continue tracing ownership all the way up the ownership chain until it identifies all individuals who own or control at least 25 percent of the LFI's customer. If the LFI has followed the steps described above and is still not confident that it has identified the individuals who truly own or control the customer, or when other high-risk factors are present, the LFI should consider intensifying its efforts to identify the UBOs. The most common method of doing so for a legal person is to identify additional UBOs below the 25 percent ownership threshold mandated by UAE law. This may involve identifying and verifying the identity of UBOs at the 10 percent or even *de minimis* percentage thresholds, as risk warrants. It may also involve requiring the customer to provide the names of all individuals who own or control any share in the customer—without requiring them to undergo CDD/KYC—in order to conduct sanctions screening or negative news checks.

In case of companies listed on a regulated stock exchange and their majority-owned subsidiaries, it is not necessary for LFIs to identify and verify the identity of a shareholder or UBO, if such information is obtainable from reliable sources, such as exchange-mandated periodic disclosure. However, an LFI may choose to prescribe in its procedures high-risk scenarios where such identification and verification should take place using either documentary or non-documentary means (for example, in case of companies listed on exchanges in jurisdictions subject to targeted financial sanctions ("TFS") or where negative news screening indicate recent changes in the status or ownership of the legal person customer).

UBOs should generally be identified and verified prior to establishing a business relationship, conforming to the same requirements and expectations that apply to the identification and verification of natural person customers, as set forth in section 3.2.1 above. Consistent with those requirements and expectations, including Article 4.3 of the AML-CFT Decision, in exceptional circumstances, where there is no ML/TF/PF suspicion and ML/TF/PF risks are assessed to be low, an LFI may complete verification after establishing a business relationship, as set forth in section 3.5 below. Further information can be found in the CBUAE's

AML/CFT Guidelines for Financial Institutions, sections 6.3.1 and 6.3.3,[9] and *Guidance for LFIs Providing Services to Legal Persons and Arrangements*.[10]

3.3. Establishing a Risk Profile

LFIs should understand the ML/TF/PF and other financial crimes risks of its customers, also known as a **risk profile** of a customer, and should reflect this risk through assigning a customer risk rating. Informed by the nature, size and complexity of their business and their types of customers, LFIs should develop a customer risk rating model that, at a minimum, meets the customer risk assessment model provisions provided for in the AML/CFT/CPF Laws, Decisions and Guidance of UAE. Additionally, as the assessment of customer risk is LFI-specific, it should also be based on the analysis of all relevant customer information. LFIs must consider the ongoing publication of information by the CBUAE and other UAE competent authorities to identify, assess, and understand the risks associated with their customers.

At the same time, an LFI's customer risk rating model should be sufficiently detailed to distinguish between variations in ML/TF/PF and other financial crimes of its customers. If such a model is improperly designed or implemented, it can have a significant detrimental impact on the LFI's ability to implement other internal controls and result in an overall weak AML/CFT compliance program. LFIs are reminded, that each customer's ML/TF/PF risk profile is dynamic and subject to change depending on numerous factors, including (but not limited to) the discovery of new information or a change in behavior, and the appropriate level of due diligence should be applied in keeping with the specific situation and risk indicators identified. In that regard, LFIs should always be prepared to increase the type and level of due diligence exercised on a customer of any ML/TF/PF risk category whenever the circumstances require, including situations in which there are any doubts as to the accuracy or appropriateness of the customer's originally designated ML/TF/PF risk category. This means that the CDD measures are not to be taken as a static formula but that depending on the risk of a customer the intensity and depth of the CDD measures should vary.

The factors used to create a customer risk profile are substantially similar to the risk categories an LFI uses when assessing its overall risk profile. Thus, an LFI should consider the following risk categories of a customer relationship:

- Products and services;
- Geographic locations; and
- Customer's type of business, customers, and counterparties.

To allow it to establish a proper customer risk profile, and as required under Article 8 of the AML-CFT Decision, LFIs should understand the nature of the customer's business and the nature and purpose of the LFI's relationship with the customer, including the expected uses to which the customer will put the LFI's products or services. One element is the collection and assessment of the customer's ownership structure

[9] Available at https://www.centralbank.ae/media/zhqjanp0/cbuae-guidelines-on-aml-cft-for-fis-june-2021_1.pdf
[10] Available at https://www.centralbank.ae/media/0yljawmh/outreach-presentation-cbuae-amlcft-guidances-for-lfis-prov-serv_-to-lp-la-and-real-estate-and-pms-sectors-4-august-2021.pdf

and UBOs, described in section 3.2.5. In addition, an LFI should collect and document the following types of information for all types of customers as part of the customer onboarding process:

- Nature of customer contact and stated purpose of the account;
- Source of funds and source of wealth;
- Customer occupation (for individual customers) or legal entity type and industry (for legal entity customers);
- Anticipated channels for maintaining the relationship (in-person, telephone, online banking, acting via an authorized representative);
- Anticipated products and services to be used throughout the relationship;
- Anticipated geography of customer's expected activity; and
- Anticipated types and volumes of transactions.

The level and type of other customer information an LFI considers collecting for the purpose of establishing a customer risk rating should correspond with its preliminary assessment of the customer's risk profile. In other words, an LFI's efforts to understand its customer should both reflect and influence the customer risk rating. If an LFI anticipates that a customer has a higher-risk profile, then it should obtain more customer information while, on the contrary, an LFI may determine that less information is required for customers with a lower-risk profile.

For example, inherently, an individual-citizen of the UAE who wishes to open a checking account to collect their salary and make ordinary day-to-day payments will typically represent a lower-risk profile than a branch of a multinational corporation wishing to open an operational account for multiple cross-border payments. Thus, for lower-risk customers, where the LFI may have an inherent understanding of the nature and purpose of the customer risk profile based on the documentation obtained at account opening, there may be no need to collect any further information. The LFI should, however, implement ongoing monitoring even for low-risk customers to ensure that their actual activity corresponds with their expected activity, stated purpose of the account, and nature of the relationship.

On the other hand, the higher the anticipated customer risk profile is, the further the LFI should consider collecting additional detailed information about:

- Source of funds ("SoF") and SoW;
- Detailed description of a customer's business operations;
- Anticipated size and/or turnover of a customer's account balances;
- Known or anticipated countries in which the customer will be transacting;
- Known or expected counterparties with whom the customer conducts transactions; and
- Anticipated timing or seasonal adjustments to a customer's transactional activity.

Obtaining a sufficient understanding of its customers and the nature and purpose of the customer relationship—together with the ongoing analysis of actual customer behavior and the behavior of relevant peer groups—allows the LFI to develop a baseline of normal or expected activity for the customer, against which unusual or potentially suspicious transactions can be identified. This element of CDD/KYC also informs the LFI's risk-based ongoing monitoring of the customer (see section 3.4) and determining whether SDD or EDD measures may be warranted (see sections 3.5 and 3.6, respectively).

3.3.1. *Customer Segmentation*

Customer segmentation involves obtaining sufficient information to assign a customer to a customer segment and to calculate an initial risk rating using the LFI's customer risk rating model. The customer segmentation process enables LFIs to appropriately divide customers into categories of risk for defining and calibrating subsequent internal FCC monitoring controls, such as determining whether the customer is subject to EDD, setting up transaction monitoring thresholds, and identifying the customer's periodic review schedule. Customer segmentation also enables an LFI to detect unusual or potentially suspicious activity if the customer engages in a transaction that deviates from what is expected for that particular customer type.

LFIs are encouraged to utilize a wide range of data elements collected as a part of baseline CDD/KYC when developing a customer risk rating and segmentation methodology. A customer's assignment to a given customer segment may automatically result in an elevated customer risk rating and thus trigger EDD and/or specific additional EDD based on the customer's industry or customer type.

3.3.2. *Source of Funds and Source of Wealth*

If an LFI determines that a particular customer represents a higher-risk relationship and warrants EDD, the LFI should use reasonable means to collect information regarding the customer's SoF or SoW.

- Identifying the SoF means to identify the direct source of the funds that are used to initially fund a customer's account, and any funds that are transacted through the account during the course of the business relationship (such as the customer's salary or the sale of a real estate property).
- Identifying the SoW means to identify the sources that have generated or significantly contributed to the customer's total net worth (such as a customer's inheritance). Where the size of balances in the account is inconsistent with a customer's stated SoW and/or where the initial source of capital for an account is unclear, LFIs should take additional steps to corroborate SoW.
- LFIs should verify the SoF/SoW by obtaining evidence from the customer, with verification requirements increasing relative to customer risk (e.g., customer statements as to employment and income sufficing for lower risk customers and bank or brokerage account statements, housing deeds, or signed court rulings indicating a customer is due compensation for those deemed higher risk).

- Depending on an LFIs risk tolerance and risk management framework, an LFI can also develop policies and procedures that require low and medium risk customers to provide evidence of SoF/SoW.
- For low risk customers, LFIs may consider obtaining information on the source of funds only.

LFIs should take a critical approach towards assessing and verifying SoF or SoW of a customer, particularly in highest-risk customer relationships. Examples of red flags that an LFI should be aware of include:

- Generic description of SoF or SoW as “inheritance,” “salary,” “income,” “investment,” “self-funding” where customer is unable to provide supporting documentation;
- Apparent inconsistencies in the stated SoF or SoW with the customer profile, such as a newly formed legal entity customer with little or no business history is funding an account with significant funds, or an unemployed customer is frequently depositing large sums;
- SoF or SoW supporting documentation has an opaque ownership structure with multiple ownership layers that lacks a clear rationale;
- Customer identified as a PEP deposits significant funds greatly exceeding their stated salary;
- Customer states that the account will be funded from a third party with no apparent links to the customer;
- Customer indicates that they will transfer the funds from another LFI to close their account;
- Customer wishes to use multiple bank accounts to fund the newly opened account with no apparent business purpose; or
- Funds will be deposited from high-risk countries or countries subject to TFS.

3.3.3. *Expected Activity*

Collecting information regarding a customer’s expected account activity and assessing self-reported expected activity is required for LFIs in order to determine the reasonableness of certain transactions. This can be completed, for example, by comparing activity against a customer’s stated purpose of the account and the transactional activity profile of the customer’s customer type or relevant peer group.

Where a customer’s self-reported expected activity appears to be inconsistent with the stated purpose of the account, or where there is a material discrepancy between the self-reported expected activity and the typical activity of the customer’s peers, LFIs should conduct an additional transaction analysis and collect sufficient information, such as a written explanation from the customer, supporting business documentation, or past financial statements, to understand and corroborate the self-reported activity.

3.3.4. *Geographic Information and Assessment of Risks*

A geographic component represents an important part of the overall customer risk rating and assessment and should be used when developing a customer risk rating methodology. LFIs should collect and assess the following types of information:

- Jurisdictions where a customer (including any of its related parties or corporate subsidiaries) resides, is registered in, or doing business in or with,
- Jurisdiction(s) of customer's counterparties; and
- Jurisdictions with which the customer expects to transact.

It is important to assess this information for any high-risk indicators such as follows:

- Presence in or operations with countries with weak regulatory AML/CFT frameworks, as determined by the LFI or as notified by local regulatory or supervisory authorities;
- Presence in or operations with jurisdictions subject to a call for action or under increased monitoring by FATF;
- Jurisdictions subject to TFS or other international sanctions;
- Other indicators of risk in a jurisdiction, such as operates in or does business with a jurisdiction that has relatively higher levels of corruption or organized crime, PF, or is known as a financial secrecy or tax haven; and
- Any discrepancies between the location where a customer seeks to open an account and its business activities (e.g., a customer is seeking to open a UAE-based account while not conducting any business activities or residing in the UAE).

3.3.5. *Prohibited Customers*

It is important for LFIs to clearly document their risk appetite, also referred to as a customer acceptance policy, that formalizes the LFI's posture toward both prospective and current customers. This customer acceptance policy typically identifies the types of customers an LFI will not accept as a matter of policy due to unacceptable legal, regulatory, or reputational risks they pose to the LFI. Thus, LFIs should develop procedures that enable employees to appropriately identify such types of customers and prevent them from onboarding or continuing an existing customer relationship with the LFI. Several examples of such potentially prohibited customers may include the following customer types (although the list is not exhaustive):

- Persons wishing to operate an anonymous account;
- Persons refusing to provide requested CDD/KYC documentation or assist in a CDD/KYC process;
- Persons subject to TFS;
- Shell banks;

- Customer where the LFI is unable to identify the UBO(s);
- Companies issuing bearer shares or owned, in whole or in part, by nominee shareholders;
- Entities the LFI determined are operating in a jurisdiction without an appropriate license or registration; or
- Persons who are the subject of material negative news (such suspected of conducting cyber-attacks and associated extortion, or suspected of illegal trafficking (human trafficking, narcotics, illegal wildlife trafficking)).

3.4. Ongoing Monitoring

Under Article 7 of the AML-CFT Decision, all customers must be subject to ongoing monitoring throughout the business relationship, as an element of both continuous CDD/KYC and suspicious activity reporting. Ongoing monitoring ensures that the account or other financial service is being used in accordance with the customer profile developed through CDD/KYC during onboarding, and that transactions are normal, reasonable, and legitimate. Depending on the nature, size and complexity of the business, LFIs can use automated, manual or a combination of both, monitoring systems and processes to conduct ongoing monitoring. However, bigger LFIs are recommended to use automated transaction monitoring systems.

3.4.1. *Risk-Based Periodic and Event-Driven Reviews*

As a part of the ongoing monitoring process, LFIs should develop standards and procedures outlining the frequency and process of periodic customer reviews, driven by the assigned customer risk rating. For example, an LFI with three customer risk categories of high, medium, and low may establish periodic reviews at the following risk-based intervals: (1) annually for customers rated as high risk; (2) every two years for customers rated as medium risk; and (3) every three years for customers rated as low risk. LFIs should ensure they have procedures and systems in place to track and monitor the progression of periodic customer profile review that are in-process. These customer risk categories and the associated periodic review schedule are not mandatory, and instead, an LFI should develop appropriate parameters for both depending on its overall ML/TF/PF risk assessment.

In addition, LFIs should perform event-driven periodic reviews upon the occurrence of a material change to the customer's profile or other "trigger" event related to the customer, including but not limited to:

- A change in a customer's domicile;
- A change in a customer's legal name through mergers and acquisitions;
- A regulatory filing (e.g., a STR) or inquiry involving a customer;
- Customer transactions are found to have been frequently rejected or blocked by correspondent banks;
- expiration of customer identification documents

- A customer requests to use higher-risk products and services or products or services that are inconsistent with the customer's business;
- Significant and unexplained changes in account activity;
- Changes in employment or business operation;
- Changes in ownership of a business entity;
- LFI employees become aware that the customer information is outdated or incorrect; or
- Customer produces a true hit against an applicable sanctions, PEP, or negative news screening list.

An LFI may prescribe in its procedures whether an event-driven review re-sets the anniversary date from when the next scheduled periodic review is to be conducted, or whether this "off cycle" event-driven review does not affect the previously scheduled periodic review date.

Both scheduled and event-driven periodic reviews consist of a refresh and assessment of customer data, documents, and risk ratings, including EDD, if applicable. As part of scheduled and event-driven periodic reviews, if a customer's CDD/KYC information has changed, information should be re-validated as correct and up-to-date and signed-off by a designated representative, as necessary.

LFIs should prescribe the processes for conducting a refresh of a customer's CDD/KYC information to address the following:

- Requesting, reviewing, and updating identification information for the customer, UBO(s), and natural person(s) acting on behalf of the customer;
- Conducting an activity review to ensure that the stated/expected activity continues to align with the actual account activity;
- Collection, verification, and review of any EDD, as required;
- Appropriate levels of manager sign-offs in case of a revised customer risk rating following the refresh; and
- Re-screening the name of the customer, UBO(s), natural person(s) acting on behalf of the customer, and other related parties as identified in section 3.8 *Name Screening*.

As outlined in the general principles of CDD/KYC, LFI should not maintain relationships with customers who are unable or unwilling to provide required CDD/KYC or EDD information during periodic review processes. If a periodic review identifies any red flags—such as apparently false information or documentation; discrepancies between the information obtained by the customer and information obtained during the verification process; lack of business justification for a complex ownership structure; or inexplicable volume/value of funds transfers—the LFI should prescribe appropriate escalation channels to investigate the activity and determine whether there are sufficient grounds for filing an STR or SAR. Where

discrepancies or red flags cannot be resolved, the account should be rejected or restricted and closed in a commercially reasonable manner.

3.4.2. *Incorporation of the Customer Risk Profile into Transaction Monitoring*

Both CDD/KYC and transaction monitoring work together and help an LFI form an understanding of their customers. CDD/KYC establishes a customer's risk profile and expected activity against which an LFI can review a customer's actual activity to assess potential variances. Transaction monitoring helps LFIs validate and continue to assess a customer's risk profile on a customer-by-customer and institution-wide basis. Transaction monitoring also feeds an LFI's suspicious activity reporting program and wider AML/CFT compliance program with information by flagging high-risk and potentially suspicious transactions and typologies.

As a basis for an LFI's transaction monitoring program and in accordance with a risk-based approach, LFIs should use a customer's risk profile to inform the degree and nature of transaction monitoring that the LFI applies to its customers. For customers identified as high risk, LFIs may choose to conduct enhanced transaction monitoring. The specific form of enhanced monitoring applied to a high-risk customer will depend on the particular circumstances of the customer relationship. For example, an LFI may set lower alert thresholds for customers who are new to the LFI.

Additionally, an LFI may apply enhanced monitoring on customers who were previously the subject of a STR or SAR filing and suspected of or investigated for potentially suspicious activity. In the case of customers that are identified as low risk, LFIs may consider monitoring and reviewing transactions at a reduced frequency and/or setting lower alert thresholds within their automated transaction monitoring program.

3.4.3. *Use of Digital Identification Systems for Ongoing Monitoring*

As discussed in section 2 of the CBUAE's *Guidance for LFIs on Digital Identification for Customer Due Diligence*, authentication using a digital identification system establishes confidence that the person asserting identity today is the same person who previously opened the account or other financial service and is, in fact, the same individual who underwent reliable, independent identification and verification at onboarding. In other words, ongoing digital authentication of the customer's identity links that individual with their financial activity. LFIs that use digital identification systems to authenticate the identity of their existing customers as part of account authorization should leverage the data both generated by authentication and other related information (such as geolocation or IP addresses) to support ongoing due diligence and transaction monitoring. For example, an LFI can use a customer's IP address to identify cases in which a customer may be transacting from a sanctioned, otherwise prohibited, or high-risk jurisdiction. Information generated from an LFI's digital identification systems therefore can be used as part of ongoing monitoring to assess whether a customer's actual activity conforms to the LFI's expectations of normal or typical activity for that customer.

3.5. Simplified Due Diligence for Lower-Risk Scenarios

As per Article 4.3 of the AML-CFT Decision, an LFI may perform SDD measures in relation to a customer, a beneficial owner of a customer, a natural person appointed to act on behalf of a customer, or a beneficiary or other payee if it is satisfied that the risks of ML/TF/PF are low. The assessment of low risks should be supported by an adequate analysis of risks by the LFI, and the selection of simplified measures should be commensurate with the type and level of risk identified through such risk analysis. In all cases, the LFI should document the details of its risk analysis and the nature of the SDD measures employed.

Where no other countervailing risk factors are present, examples of potentially lower-risk scenarios may include those in which:

- The customer is a UAE government entity, including UAE state-owned enterprises;
- The customer is an entity listed on a stock exchange and subject to regulatory disclosure requirements that identify a customer's UBOs; and
- The customer is rated as low risk under the LFI's documented customer risk rating methodology.

Where an LFI is satisfied that the ML/TF/PF risks are low, the LFI may perform one or more of the following SDD measures, as warranted by the risk analysis:

- Verifying the identity of the customer and any UBO(s) after establishing the business relationship, provided verification is nonetheless completed in a timely fashion (to be documented in the LFI's internal procedures) and appropriate controls are in place to manage the ML/TF/PF risks associated with the customer and the relationship prior to verification;[11]
    - Note that, even where identity verification may be postponed until after the establishment of a business relationship, LFIs should nonetheless obtain basic identifying information (on both natural person and legal entity customers) prior to the establishment of any business relationship.
- Reducing the frequency of updates to CDD/KYC information;
- Reducing the degree of ongoing monitoring and scrutiny of transactions, based on a reasonable monetary threshold; or
- Developing an understanding of the intended nature and purpose of the customer relationship on the basis of the relationship type and the customer's historical transaction activity, rather than by collecting information regarding the intended nature and purpose of the relationship during onboarding or at a periodic or event-driven CDD/KYC refresh.

An LFI should not perform SDD measures where:

- A customer or any UBO of the customer is from or in a country or jurisdiction identified as non-cooperative by the FATF;

[11] Such measures may include holding funds in suspense or escrow until verification of identity has been completed or making completion of identity verification a precondition of closing any transaction with or on behalf of the customer.

- A customer or any UBO of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the LFI, or as notified by local regulatory or supervisory authorities; or
- The LFI suspects that ML, TF, or other criminal activity is involved.

3.6. Enhanced Due Diligence for Higher-Risk Scenarios

The AML-CFT Law and the AML-CFT Decision impose specific and EDD obligations on LFIs with respect to three classes of customers or transactions:

- Customers that are foreign or domestic PEPs, which include the direct family members or associates known to be close to the PEPs (AML-CFT Decision, Article 15); and
- Business relationships and transactions with natural persons, legal persons, or legal arrangements from high-risk countries (AML-CFT Decision, Article 22).

The AML-CFT Law and AML-CFT Decision give special attention to customers in these groups because they are likely to expose LFIs to a heightened risk of money laundering, terrorist financing, and other financial crimes.

In addition to these classes of customers and transactions, for which EDD is mandatory, LFIs are expected to implement appropriate policies and procedures to determine whether relationships with or transactions undertaken for or on behalf of a customer present a higher risk for money laundering or terrorist financing, and thus whether the customer warrants EDD. Examples of potentially higher-risk scenarios include, but are not limited to, those in which:

- The customer belongs to a higher-risk industry or sector identified in topical risk assessments, or to an industry or sector identified by the LFI as higher-risk for money laundering or terrorist financing;
- The ownership structure of a legal entity customer appears unusual or excessively complex given the nature of the legal entity's business;
- The legal entity customer is a personal asset-holding vehicle;
- The business relationship is conducted under unusual circumstances, such as significant unexplained geographic distance between the LFI and the customer;
- The legal entity customer has nominee shareholders or shares in bearer form;
- The customer is a cash-intensive business or conducts cash-intensive operations;
- The customer performs complex operations that do not have clear economic objective;
- The customer has a presence in or operations with countries with weak regulatory AML/CFT frameworks, as determined by the LFI or as notified by local regulatory or supervisory authorities;

- The customer operates in or does business with a jurisdiction that has relatively higher levels of corruption or organized crime, or is known as a financial secrecy or tax haven;
- The relationship involves or could involve cash or anonymous transactions;
- The relationship involves or could involve frequent payments received from unknown or unassociated third parties.

As per Article 4.2(b) of the AML-CFT Decision, where the LFI identifies a customer or relationship as presenting higher ML/TF/PF risks, it must apply EDD measures commensurate with those risks. Examples of EDD measures include but are not limited to:

- Obtaining approval from the LFI's senior management to establish or continue a business relationship with the customer;
- Establishing the SoF and SoW of the customer and any UBO of the customer;
- Conducting enhanced monitoring during the course of the business relationship with the customer, including by increasing the degree and nature of transaction monitoring and CDD/KYC updating;
- Requiring the first payment to be carried out through an account in the customer's name with an LFI subject to similar or equivalent CDD/KYC standards;
- Using public or private sources of information (e.g., websites, proprietary databases) to gain a better understanding of the reputation of the customer or any UBO of the customer;
- Commissioning external intelligence reports where it is not possible for the LFI to easily obtain information through public sources or where there are doubts about the reliability of public information; and
- For high net-worth individuals, particularly those utilizing higher-risk products or services or characterized by other markers of heightened ML/TF/PF risk:
    - Independently corroborating information obtained on the SoF and SoW of customers and UBOs against documentary evidence or public information sources;
    - Screening operating companies and individual benefactors contributing to the customer's and UBOs' SoF and SoW; and
    - Scrutinizing transactions relating to customers that have multiple accounts with the LFI or to customers having a common beneficial owner.

In addition, as noted in section 3.2 *Customer and Beneficial Owner Identification and Verification*, if the LFI has followed its standard beneficial ownership identification and verification procedures and is still not confident that it has identified the individuals who truly own or control the customer, or when other high-risk factors are present, the LFI should consider intensifying its efforts to identify the UBOs. The most common method of doing so is to identify additional UBOs below the 25 percent ownership threshold mandated by UAE law. This may involve identifying and verifying the identity of UBOs at the 10 percent or even *de*

minimis percentage thresholds, as the customer's risk warrants. It may also involve requiring the customer to provide the names of all individuals who own or control any share in the customer—without requiring them to undergo CDD—in order to conduct sanctions screening or negative news checks.

Additional examples of EDD measures are provided in the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 6.4.[12]

3.7. Non-Face-to-Face Relationships

LFIs should develop policies and procedures to address any specific risks associated with non-face-to-face customer relationships and transactions undertaken in the course of such relationships. Such policies and procedures should be applied when establishing a new customer relationship and when conducting ongoing monitoring and should be at least as stringent as those that would be required to be performed if there was face-to-face contact. Note that relationships in which personal contact between a representative of the LFI and the customer is achieved via video teleconference are not considered to be non-face-to-face relationships for the purpose of this Guidance.

Heightened ML/TF/PF risks may arise from establishing business relationships or undertaking transactions according to instructions conveyed by customers over the internet (absent personal contact via video teleconference), digital application, post, fax, or telephone. An LFI should note that online applications and transactions may pose greater risks than other non-face-to-face business due to the following factors, which taken together may compound the associated ML/TF/PF risks:

- The ease of unauthorized access to the application or online banking platform, across time zones and locations, in situations where third persons received or have stolen customer's log-in credentials;
- The ease of making multiple fictitious applications or requests without incurring additional cost or the risk of detection;
- The ease of concealing a customer's residence in a country subject to TFS;
- Individuals being used as a "front" for an unknown third party;
- The absence of physical documents; and
- The speed and often irreversible nature of electronic transactions.

The measures taken by an LFI for verifying the identity of customers and UBOs in the context of non-face-to-face relationships will depend on the nature and characteristics of the product or service provided and the customer's risk profile. Where verification of identity is performed without face-to-face contact (e.g., electronically), an LFI should apply additional checks to manage the risk of impersonation or fraud. The additional checks may consist of robust anti-fraud checks that the LFI routinely undertakes as part of its existing procedures, which may include as appropriate and feasible:

[12] Available at https://www.centralbank.ae/media/zhgjanp0/cbuae-guidelines-on-aml-cft-for-fis-june-2021_1.pdf

- Telephone contact with the customer at a residential or business number that can be verified independently;
- Confirmation of the customer's address through an exchange of correspondence or other appropriate method;
- Subject to the customer's consent, telephone confirmation of the customer's employment status with his or her employer's human resource department at a listed business number of the employer;
- Confirmation of the customer's salary details by requiring the presentation of recent bank or payment statements where applicable;
- Provision of certified identification documents by lawyers or public notaries;
- Requiring the customer to make an initial payment using a check drawn on the customer's personal account with a bank in the UAE;
- Requiring customers to use multi-mode authentication factors for access to online banking or digital applications; and
- Conducting a video call with the customer.

When engaging in non-face-to-face relationships, LFIs should continue to explore digital identification systems that can enable remote customer identification and verification, support remote financial transactions, and otherwise facilitate non-face-to-face business relationships and transactions, please see section 3.2.4.1 *Digital Identification and Verification.* Given the evolution of digital identification technology and the emergence of consensus-based open-source digital ID technical standards, non-face-to-face interactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place may present a standard level of risk, and may even present a lower level of risk where higher assurance levels are implemented and/or appropriate control measures are present.

See the CBUAE's *Guidance for LFIs on Digital Identification for Customer Due Diligence*, section 4 for specific risk mitigation measures and strategies that can help ensure that a digital identification system is suitably "reliable" and "independent" in this sense.

3.8. Name Screening

An LFI should screen the following parties against relevant ML/TF/PF information sources (such as negative media databases), databases of known PEPs, and internal watchlists (such as lists of customers previously exited or denied onboarding for financial crime reasons) prior to a customer's onboarding and keep records of true matches as part of the KYC documentation:

- All customers, regardless of risk rating or risk profile;
- UBOs of legal entity customers;
- Natural persons appointed to act on behalf of the customer (see section 3.2.3);

- Names of relevant persons holding senior management positions with the legal person (such as directors, partners, authorized signatories, and managers); and
- Natural persons having executive authority over customers that are legal arrangements.

All LFIs are required to fully comply with the obligation to implement all necessary measures without delay as described in the Cabinet Decision No. (74) of 2020, Executive Office for Control & Non-Proliferation ("EOCN")'s *Guidance on Targeted Financial Sanctions for FIs, DNFBPs, and VASPs*[13] and the CBUAE's *Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions*, and *Guidance for Licensed Financial Institutions on Transaction Monitoring Screening and Sanctions Screening.*[14]

This means that all LFIs must maintain awareness of sanctions promulgated by the UNSC as well as the UAE sanctions list(s) published on the EOCN's website. In addition, LFIs must register on the EOCN's website to receive automated email updates about changes to the UAE sanctions list.

With respect to these sanctions lists, the parties listed above must be screened prior to a customer's onboarding and on an ongoing basis thereafter. The results of screening and assessment by the LFI should be documented. When there is a confirmed match against an existing customer, an LFI must freeze without delay (within 24 hours) all funds and other assets. When a partial name match is identified, the LFI is required to suspend without delay any transaction and refrain from offering any funds, other assets, or services. In case of confirmed or partial name match for a potential customer, the LFI should reject the customer and refrain from offering any services. An LFI must report all confirmed or potential matches, for existing and potential customers, in addition to the actions the LFI has taken to suspend or freeze the relevant funds or transactions, as required, utilizing the UAE FIU's online reporting platform, goAML, within five business days of the required action taken.

3.9. Customer Rejection and Exit

Under Article 14.2 of the AML-CFT Decision, LFIs should not deal with any person on an anonymous basis or any person using a fictitious name and using pseudonyms, fictitious names, or numbered accounts without the account holder's name. In addition, as outlined in section 3.3.5 *Prohibited Customers*, an LFI may decide that certain types of customers are outside of its risk appetite and should not be onboarded or that ongoing relationships with such customers should be terminated.

Prior to establishing a business relationship, if an LFI has any reasonable grounds to suspect that the assets or funds of a customer are the proceeds of crime or related to the financing of terrorism, the LFI should reject the business relationship and, per Article 17 of the AML-CFT Decision, file an STR or SAR with the UAE FIU.

[13] Available at: https://www.uaeiec.gov.ae/API/Upload/DownloadFile?FileID=7f006d28-4a65-4829-aa35-b9dc3059e89a.
[14] Available at: https://www.centralbank.ae/en/cbuae-amlcft

As per Article 13.1 of the AML-CFT Decision and Article 15 of Cabinet Decision 74, if an LFI is unable to undertake the CDD/KYC measures described in this Guidance, or identifies a confirmed match to a party included on applicable sanctions lists, the LFI must:

- Not onboard the customer;
- In case of a confirmed match, freeze without delay and without giving a notice to the customer, funds owned or controlled, wholly or jointly, directly or indirectly, by a sanctioned person or by a person or organization acting on behalf of or at the direction of a sanctioned person;
- Exit the relationship if one has been established;
- For insurance operators, not make any payment to a payee or beneficiary under the customer's policy or other insurance relationship; and
- Maintain all related records (see section 4 *Record-keeping* below).

In addition, the LFI may decide to add the customer, its UBOs, directors, and managers to the LFI's internal watchlists to ensure the individual is prevented from being onboarded with the LFI in the future. The LFI should also determine whether the circumstances warrant the filing of an STR or SAR. The LFI is required to document the customer rejection or exit rationale(s) as well as the exit policy and procedures.

3.10. Third-Party Reliance

Third-party reliance enables an LFI to rely on the CDD measures carried out by another LFI that is regulated in the UAE, or an equivalent entity regulated under a foreign law that adheres to the CDD and record-keeping requirements outlined in the AML-CFT Decision. LFIs are permitted to rely on certain third parties – financial institutions or designated non-financial businesses and professions ("DNFBPs") – to perform the following elements of CDD measures:

a) Identifying a customer and verifying a customer's identity using reliable, independent source documents, data, or information.

b) Identifying a beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that an LFI is satisfied that it knows the identity of the beneficial owner.

c) Understanding and obtaining information on the purpose and intended nature of the business relationship.

When entering into a third-party reliance arrangement, LFIs should ensure the third party has appropriate measures in place to comply with the UAE's AML/CFT regulatory requirements. LFIs should ensure that the following criteria are met:

a) An LFI relying upon a third party should immediately obtain the necessary information concerning elements (a) to (c) as outlined above, as well as all other identification data and necessary information collected during the CDD.

b) LFIs should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

c) LFIs should satisfy itself that the third party is regulated, supervised or monitored for ML/TF/PF compliance, and adheres to the CDD and record-keeping requirements outlined in the AML-CFT Decision.

d) When determining in which countries the third party that meets the conditions can be based, LFI should have regard to information available on the level of country risk.

The third-party reliance does not apply in the context of outsourcing, service provider, or agency relationship. The third-party reliance is only acceptable in the case of reliance on other financial institutions or DNFBPs conducting CDD, which typically means that the third party will have an existing business relationship with the customer, which is independent from the relationship to be formed by the customer with the relying financial institution. In contrast, in the scenario in which the outsourced entity applies the CDD measures *on behalf of* the delegating financial institution, in accordance with its procedures, the delegating LFI must ensure control of the effective implementation of its CDD procedures by the entity/agent.

The AML-CFT Decision Article 19 states that even in situations where reliance on third parties is permitted, the ultimate responsibility for CDD measures remains with the LFI relying on the third party. Therefore, third-party reliance in no way relieves the relying LFI of performing other CDD measures, including understanding a customer's expected activity, determining whether customers are high-risk, and assessing whether a customer's transactions constitute suspicious activity.

LFIs that decide to utilize reliance on third parties should develop clear policies and procedures outlining when it is acceptable to do so and what steps an LFI's staff should follow to satisfy themselves that the requirements in sections (a)-(d) above are met.

Whichever methods are utilized, LFIs bear the ultimate responsibility of ensuring that the third parties adhere to the statutory CDD and record-keeping requirements of the UAE, and that the CDD documentation provided are complete, adequate, valid, authentic, and meets the UAE AML/CFT/CPF requirements.

An LFI should conduct sample tests from time to time to ensure CDD information and documentation is produced by the third-party upon demand and without undue delay.

Whenever an LFI has doubts as to the reliability of the third-party, it should take reasonable steps to review the third-party's ability to perform its CDD duties. If the LFI intends to terminate its relationship with the third-party, it should immediately obtain all CDD information from the third-party. If the LFI has any doubts regarding the CDD measures carried out by the third-party previously, the LFI should perform the required CDD as soon as reasonably practicable.

Best Practices for Third-Party Reliance

- The relying LFI and the third party should have an agreement in place (such as a service-level agreement) that acknowledges the existence of reliance and outlines its major principles and considerations, including the roles and responsibilities of the LFI and the third party and the nature of the CDD and record-keeping requirements to be fulfilled by the third party.
- Third-party reliance arrangements should be approved by an appropriate senior managing official within the LFI.
- The LFI's policies and policies should document the third-party reliance arrangement and should establish review procedures for evaluating the relationship on an ongoing basis, including the adequacy of the third party's CDD and record-keeping measures.
- LFIs should conduct a periodic review of the third party to ensure that it continues to conduct CDD and record-keeping in a manner as comprehensive as the LFI and is consistent with the UAE's AML/CFT regulatory requirements.
- The LFI should assess negative news and any enforcement action regarding AML/CFT deficiencies or violations involving the third party to determine whether it should engage or continue to engage in a third-party reliance arrangement with the entity.
- The LFI's risk assessment should identify reliance on third parties and evaluate the risk exposure posed by the LFI's third-party reliance arrangements.
- LFIs should consider terminating reliance with a third party that fails to apply adequate CDD on their customers or otherwise does not meet the LFI's AML/CFT requirements.

4. Record-keeping

According to Article 16 of the AML-CFT Law and Article 24 of the AML-CFT Decision, LFIs should maintain detailed records associated with their ML/TF/PF risk assessment and mitigation measures as well as records, documents, data, and statistics for all financial transactions, all records obtained through CDD/KYC measures, ongoing monitoring, sanctions screening, account files and business correspondence, copies of personal identification documents, and STR or SAR files and results of any analysis performed. LFIs should maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions. Records should be sufficient to permit reconstruction of individual transactions in order to provide, if necessary, evidence for prosecution of criminal activity. LFIs are also required to make records available to the competent authorities immediately upon request.

The statutory retention period for all records is at least five years, from the date of completion of the transaction; termination of the business relationship with the customer; completion of the inspection by the CBUAE; issuance of a final judgment of the competent judicial authorities; or liquidation, dissolution, or

other form of termination of a legal person or arrangement. Although the statutory retention period mandates that LFIs maintain records for at least five years, LFIs may retain records for a longer period of time at their own discretion.

Accordingly, an LFI should maintain the following types of records as part of a well-documented AML/CFT compliance program:

- **Policies and procedures**: LFIs should maintain its AML, CFT, sanctions, fraud, and other applicable policies and procedures, standard operating manuals, internal guidance, and logs documenting any changes made to these documents over time.
- **Customer information**: LFIs are generally required to verify a customer and related parties' identity before doing business with the customer and keep records of the verification process performed. As such, LFIs should maintain records related to identifying and verifying individual or legal entity customer and related parties' information, such as a customer's name, address, date of birth, and the date of a customer's incorporation.
- **Customer screening**: LFIs should maintain any records generated during screening a customer and related parties against lists of Politically Exposed Persons ("PEPs"), adverse news, and UNSC and UAE local sanctions, as well as results of any investigations or alert resolution (e.g., in case of confirmed true hits or false positives).
- **Other customer due diligence records**: LFIs should maintain records related to the CDD/KYC process, such as documents pertaining to a customer's source of wealth ("SoW"), results of internal enhanced due diligence ("EDD"), regulatory requests, and decisions to onboard or offboard a customer.
- **Documentation on third-party reliance**: LFIs should maintain policies, procedures, and service-level agreements describing an LFI's reliance on a third party to conduct CDD/KYC on the LFI's behalf, including the roles and responsibilities of the third party and the LFI's process to determine the adequacy of the third party's CDD/KYC controls.
- **Transactions**: LFIs should keep records of all transactions with their customers, including the type and amount of the transaction, the date, the parties involved, and any underlying documentation the LFI may have requested from a customer. These transactions include those executed or processed by the LFI, whether domestic or international in nature, and irrespective of the type of customer and whether or not a business relationship is maintained with the LFI.
- **External and internal compliance reports**: LFIs should prepare and maintain periodic internal compliance reports and metrics, such as results of monitoring activities, independent audit reports, risk assessments, documents related to employee background investigations (i.e., documentation of the Know Your Employee ("KYE") process), incidents or violations reports, trends in customer risk ratings, and other analysis. This extends to SAR and STR reports submitted to the FIU and supporting documentation specific to the filing, including any follow-up requests from the FIU. LFIs

should also keep detailed records of any root cause analyses and remediation actions taken to address identified shortcomings in the LFI's AML/CFT compliance program.

- **Investigation records**: LFIs should keep records of all internal investigations regarding their customers, their activities, or any red flags, including any evidence collected and the ultimate resolution.
- **Information that is not processed**: LFIs should keep records of any information they receive that is not processed or that may raise a red flag, such as customer requests for omitting or altering information to avoid scrutiny and attempted transactions.
- **Regulatory requests and remediation:** If a regulatory authority requests information from an LFI or issues an assessment report indicating deficiencies in the LFI's policies and controls, the LFI should keep records of the information provided and any actions taken as a result of the regulatory engagement.
- **Training Monitoring**: LFIs should keep records of employee training (for example, the date the training took place, a list of the participants who received the training, and the topics that were covered as part of the training). LFIs should also keep records related to the effectiveness of their training programs, such as employee test scores and feedback, to improve future training efforts.

LFIs should document in their internal procedures how they store these records and whether this takes place in a physical or digital form and whether the records stored are originals or scanned/electronic copies. For further details, see the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 9.[15]

[15] Available at https://www.centralbank.ae/media/zhgjanp0/cbuae-guidelines-on-aml-cft-for-fis-june-2021_1.pdf

Annex 1. CDD/KYC Red Flags

LFIs should establish a list of ML/TF/PF red flags associated with collecting and updating CDD/KYC information on a customer. The following is a list of representative ML/TF/PF red flags that, when identified, may warrant additional scrutiny. LFIs should tailor these ML/TF/PF red flags to their specific institution and to specific products and services that the LFI offers.

Red flags related to a customer's CDD/KYC information

- A customer provides misleading, inaccurate, or incomplete information.
- A customer's identity cannot be verified, or the customer is unable or refuses to provide all of the information and documents required by the LFI.
- There are inconsistencies in the identification documents provided by the customer, such as a customer provides onboarding documents that contain variations in the customer's name.
- A customer produces documents that appear to be counterfeited or altered.
- A customer's home or business telephone is disconnected.
- The information that is provided by a customer is inconsistent with other (publicly available) information.
- There are apparent inconsistencies in the stated SoF or SoW with a customer profile, such as a newly formed legal entity customer with little or no business history is funding an account with significant funds.
- A customer, related parties, and/or beneficial owners are associated with material negative news.
- A customer has no record of past or present employment experience.
- A customer is a trust or shell company that is reluctant to provide information on controlling parties and underlying beneficiaries.
- A business (legal entity)'s shareholder composition is overly complex.
- A customer indicates they intend to engage or are currently engaging in high-risk products or services (such as high-volume and high-value cross-border funds transfers) without a reasonable explanation.
- A customer wishes to use multiple accounts to fund the newly opened account with no apparent business purpose.
- A customer's account will be funded from a third party with no apparent links to the customer.

Red flags related to a customer's behaviour

- A customer demonstrates a defensive stance to the LFI's CDD/KYC questions.
- A business (legal entity) is reluctant to provide information about the nature of its business, anticipated account activity, prior banking relationships, the names of its related parties and UBOs, or other information as required by the LFI.

- A customer provides an insufficient explanation on their SoF and/or SoW (as “inheritance,” “salary,” “income,” “investment,” “self-funding”), or is uncomfortable providing SoF and/or SoW information to the LFI.
- A customer provides information that is misleading, inaccurate, or incomplete on its UBOs.
- A customer indicates that they intend to engage with jurisdictions that the LFI knows to be at a higher risk for ML/TF/PF or non-cooperative by the FATF.
- A customer asks to be exempted from the LFI’s reporting or recordkeeping requirements.
- A customer makes inquiries about the LFI’s AML/CFT and Sanctions Policy.

Red flags related to a customer’s transactions

- A customer’s transactions (volume or value) exceed the expected activity established at onboarding.
- There is a sudden change in the customer’s pattern of activity or transactions. For example, a customer engages in large and/or rapid movement of funds and/or rounded transactions that is inconsistent with the customer’s historical profile.
- A customer uses products or services that are unusual for that customer type. For example, the customer is a small convenience store engaging in custodial and brokerage services.
- A customer engages in transactions between parties that are not usually connected (e.g., a textile producer transacting with a luxury car dealer) and who were not disclosed to the LFI at onboarding.
- A customer’s engages in transactions inconsistent with what is expected from the customer’s expected declared business revenue or customer’s income/employment information. For example, a customer makes high-value transactions, but the LFI’s CDD/KYC information indicates the customer is unemployed.
- A customer begins to send or receive transactions to or from a financial secrecy or tax haven, or to or from a higher-risk geography which is inconsistent with the customer’s business and information provided at onboarding.
- A customer transacts outside an area near their home address, employment address, or business address which is inconsistent with the customer’s information provided at onboarding.