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

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AND ILLEGAL ORGANISATIONS

GUIDANCE FOR REGISTERED HAWALA PROVIDERS AND LICENSED FINANCIAL INSTITUTIONS PROVIDING SERVICES TO REGISTERED HAWALA PROVIDERS

August 15, 2021

Contents

Part I: Registered Hawala Providers and Licensed Financial Institutions

1 Introduction

1.1 Purpose

Article 44.11 of the *Cabinet Decision No. (10) of 2019 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") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE. 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 79/2019 dated 27/06/2019) and any amendments or updates thereof.[1] As such, while this 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, such as outreach sessions and thematic reviews conducted by the CBUAE.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices and red flag indicators. 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 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 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 licensed and/or supervised by the CBUAE in the following categories:

- Registered Hawala Providers ("RHP");
- National banks, branches of foreign banks; and
- Exchange houses.

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

Key Definitions and Acronyms

AML/CFT: Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations.

Beneficial owner: The natural person who owns or exercises effective ultimate control, directly or indirectly, over a client; 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.

Beneficiary Hawala Provider: The beneficiary's Hawala Provider, or receiving Hawala Provider, that receives the funds or equivalent value from the Originating Hawala Provider.

CBUAE Regulations: Any resolution, regulation, circular, rule, instruction, standard or notice issued by the CBUAE.

Hawala Activity: The arrangements for transfer and receipt of funds or equivalent value and settlement through trade and cash.

Hawala Provider Certificate: The Certificate issued by the CBUAE for carrying on Hawala activity in the UAE.

Legal person: Any entities other than natural persons that can establish in their own right a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, partnerships, or associations, along with similar entities.

Money or Value Transfer Service (MVTS): financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs.

Originating Hawala Provider: The originator's Hawala Provider, or sending Hawala Provider, that initiates and carries out the transfer of funds or equivalent value to the Beneficiary Hawala Provider.

Registered Hawala Provider: Any natural person holding a valid residency visa or Legal Person, who is registered in the CBUAE's Hawala Providers Register in accordance with the provisions of its Circular No. 24/2019, including its agents or a network of agents.

Registered Hawala Provider Agent: Any natural or legal person carrying out activity outside the UAE on behalf of a Registered Hawala Provider.

1.3 Legal Basis

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

- Decree Federal Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Law").
- Cabinet Decision No. (10) of 2019 concerning the Implementing Regulation of Decree Federal Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organizations ("AML-CFT Decision").
- 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, Terrorists Financing & Proliferation of Weapons of Mass Destruction, and Related Resolutions ("Cabinet Decision 74").
- Registered Hawala Providers Regulation issued by the CBUAE ("Circular No. 24/2019").

Under Articles 4 and 5 of Circular No. 24/2019, RHP and their customers and agents must strictly abide by all UAE laws, including civil laws, Commercial Companies' Law, federal laws on AML/CFT, and any Regulations and directions issued by the CBUAE ("the legal and regulatory framework in the UAE"). RHP may be guided by the FATF standards on AML/CFT and Proliferation and must abide by guidance issued by the CBUAE in this regard.

1.4 Organization of this Guidance

The FATF's Mutual Evaluation Report of the UAE issued in April 2020 stated that the MVTS sector, including the Hawala service providers, is weighted as highly important in terms of risk and materiality in the UAE. This Guidance is addressed to the i) RHP and ii) LFIs that provide accounts or financial services to RHP. Part I of this Guidance applies to both RHP and LFIs, whereas Part II applies specifically to RHP and Part III specifically to LFIs.

2 Overview of Hawala activity

The FATF defines hawala providers (and other similar service providers) as money transmitters, particularly with ties to specific geographic regions or ethnic communities, that arrange for transfer and receipt of funds or equivalent value and settle through trade, cash, and net settlement over a long period of time. While hawala providers—also known as hawaladars—often use banking channels to settle between them, what makes them distinct from other money transmitters is their use of other settlement methods, including trade, cash, and long-term net settlement.[2] Hawala is an activity based on trust and was established to avoid high charges by people who cannot afford them, the ability to reach beneficiaries in remote places quickly where banks do not operate, and the existence of strict currency controls in some countries. Because communication is often by text message and there is no need for funds to clear, hawala transfers may also be available faster than the ones made using the formal financial system. Although hawala providers generally specialize in transferring money between certain jurisdictions, they are also part of larger networks that can arrange transfers to almost any part of the world. Such transfers are likely to be slower and more expensive than transfers within the corridors in which the provider specializes. Although the hawala system minimizes use of the formal financial system, including use of international wires, it is important to note that almost all hawaladars will ultimately seek to conduct transfers, particularly international transfers through LFIs, and possibly to use other financial services. In doing so, they could expose the LFI with which they do business with to the risks of their own business activities and customers.

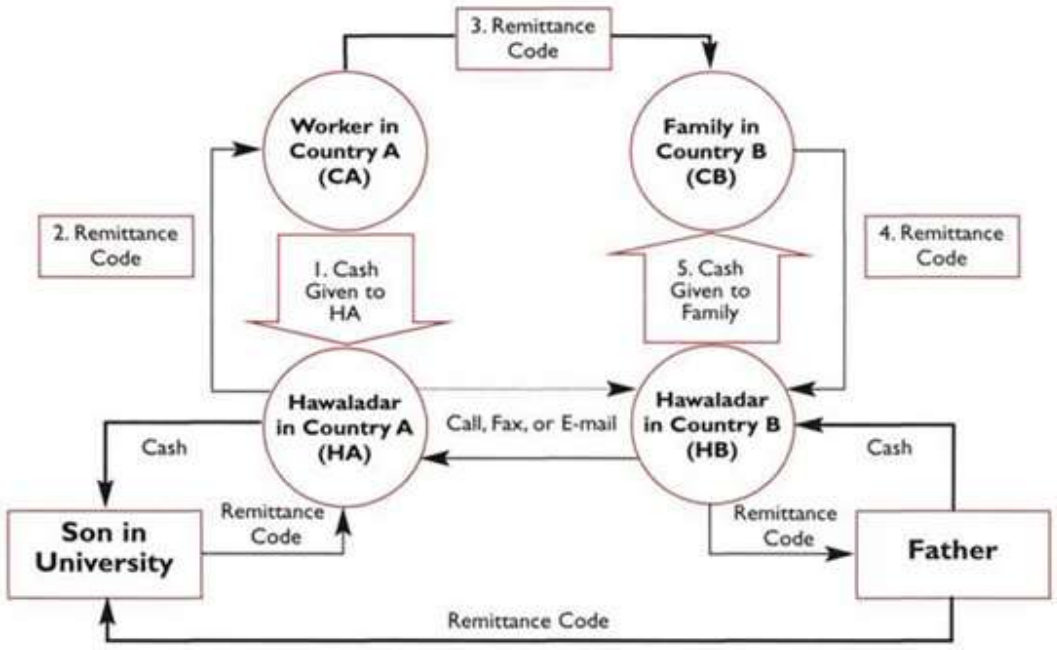
Common Attributes of Hawala Providers

- Fees for funds transfers are less than other channels and funds are available faster.
- Operates in communities in which the Hawala Provider is known, visible and accessible to the customers.
- Operates in areas with high numbers of expatriates/migrant workers of a specific ethnic group by providing cultural convenience with absence of language barriers, trust among community members, and solidarity among migrants with limited education levels and literacy.
- Operates with jurisdictions and regions underserved by other types of financial service providers, such as high-risk areas experiencing wars, civil unrest, conflicts, economic crisis, or weak or non-existent banking systems.

[2] See also the FATF report The Role of *Hawala* and Other Similar Service Providers in ML/TF (fatf-gafi.org)

- Operates as a hawala provider to facilitate remittance services as a side business to other business activities.
- Provides one-off remittance services and communicates with the customer only as much as needed to conduct the transaction.

Sample Hawala Transaction:[3]



3 Global risks of Hawala activity

Hawaladars' business model is built around satisfying customers' needs to move money rapidly across borders, a service that may also be misused by criminals as is to individuals seeking to conduct legitimate personal remittances. In recent years hawala providers have been repeatedly abused to transfer illicit funds, including funds involved in terrorist financing. Certain providers have been found to be fully complicit in these schemes, and even to operate as professional money launderers. In addition, hawala providers generally have the greatest competitive advantage in areas where more formal MVTS providers do not operate or have limited infrastructure, often because these jurisdictions are remote or classified as very high risk. Although this certainly does not mean that every transaction to those areas is illicit, it does suggest that the institutional risk profile of the average hawala provider is likely to be higher than that of other MVTS providers. In many jurisdictions, hawala providers operate *underground*, because they are providing an illegal service or because they and their customers don't want to be required to comply with rules related

[3] Source: IMF III Features of the Informal Hawala System : Informal Funds Transfer Systems : An Analysis of the Informal Hawala System: (imf.org)

to taxes, currency controls, and AML/CFT compliance. This is especially common among hawala providers operating in jurisdictions where hawala is prohibited, unregulated, or illegal.

The inherent risk of hawala providers is influenced primarily by the regulatory environment and illicit finance risks in the jurisdictions in which they do business, the products and services they provide, and their customer base:

1. Regulatory Environment

The regulatory environment for hawala providers clearly varies across jurisdictions. In some jurisdictions, they are not able to maintain a license or registration and therefore operate entirely underground. While operating underground is generally prohibited under the laws of the country where the hawala provider operates, it does not necessarily mean that a provider is a money launderer. Still, underground providers will seek to conceal their activities from financial institutions, and are extremely unlikely to comply with any AML/CFT obligations. Such entities may present themselves to LFIs as "general trading companies" or describe other business types that can justify regular international transfers, including dealing in precious metals or stones, trading in used cars, or in high value carpets.

Even in jurisdictions where hawala is legal and regulated such as the UAE, hawala providers may have only a basic understanding of their financial crime risks and obligations, and may not use systems and technologies that support compliance with those obligations. Furthermore, because hawaladars may lack strong AML/CFT preventive measures, they may be sought out by customers specifically hoping to take advantage of this possible weakness. As a result, hawala providers are almost always found to be classified as very high-risk customers by banks. **A hawala provider can strive to manage this risk by applying strong, targeted controls and maintaining an effective AML/CFT program that meets or exceeds UAE requirements and global standards** (see Part II section 3 below).

2. Geography

Hawala providers, like all financial institutions, are heavily exposed to the risks prevalent in the geographies where they operate. The risk of a hawala provider, therefore, will depend in part on the illicit finance risks—including ML/TF and sanctions evasion—in the jurisdictions where it is established or has subsidiaries. In addition, a provider's risk will also be impacted by the jurisdictions with which it most frequently does business. For example, the risk of a hawaladar operating in the UAE and primarily executing transfers to and from Country X should be assessed based on the illicit finance risk in both the UAE and Country X.

3. Products, Services, and Delivery Channels

Hawala providers, by definition, all provide money or value transfer services using hawala networks, which is subject to higher risks. The risk of hawala transactions may be increased or decreased by the size and purpose of the transaction. Some hawaladars only carry out low-value personal remittances, while others service businesses by supporting commercial operations, which may involve relatively high-value transactions. Low-value personal remittances may be considered lower-risk, although low-value remittances to jurisdictions at high-risk for terrorist financing should be treated as equally high risk. **RHP in**

the UAE may perform only limited services (listed in section 4.1 below), but hawala providers established elsewhere may not have such restrictions on their activity.

The risk involved in providing the hawala service is further impacted by the delivery channels through which it is offered. Channels that promote anonymity (accepting transaction orders by text or telephone; accepting cash; allowing agents or third parties to order transactions on behalf of the originator) increase the risk of the service. Some international law enforcement agencies have reported cases of hawala providers operating in virtual currencies; although still rare, such a delivery channel would be extremely high risk, as it would combine the general risks of hawala providers with those of virtual currencies, which offer illicit actors anonymity and access to a practically unregulated financial sector.

In addition, hawala services may not be the only financial product hawala providers offer. In many jurisdictions providers also offer small loans (often with pawned items as security) and sell stored value cards, or provide safekeeping services for cash. They may also engage in non-financial lines of business such as selling calling cards, mobile phones and SIM cards. All of these lines of business are cash intensive[4] and high-risk, and are generally not subject to AML/CFT controls. Even in a jurisdiction where hawala providers are regulated, they may commingle cash proceeds of these other services with hawala funds. This means that a hawala provider with an account at an LFI could use that account to support all aspects of its business, not simply provision of hawala services.

4. Customer Base

Most hawala providers are likely to serve a customer base made up of lower-income individuals seeking to conduct or receive fairly low-value transfers. Such a customer base is not necessarily low-risk, especially when customers have ties to jurisdictions that are at high risk for terrorist financing. The risk of the provider's customer base, however, will be further increased if the provider conducts larger transfers on behalf of business entities (e.g. trade-based transactions), if it has a high proportion of legal person customers, or if its customers include politically exposed persons.

4 Regulation and Supervision of RHP in the UAE

The CBUAE permits legitimate Hawala Activity as an important element of its continuous efforts to support financial inclusion and bring the unbanked population into the regulated financial system. To this end, Hawala is regulated by the Registered Hawala Providers Regulation issued by the CBUAE ("Circular No. 24/2019"). As per its articles 2.1 and 7.1 and Article 26 of the AML-CFT Decision, **all providers carrying on Hawala Activity in the UAE must hold a Hawala Provider Certificate issued by the CBUAE;** it is not permitted to carry on Hawala Activity without being registered with the CBUAE.

RHP are supervised by the CBUAE, who has the right to examine the business of RHP and their agents and customers whenever it deems appropriate to ensure proper compliance with their statutory obligations under the legal and regulatory framework in the UAE, or impose supervisory action or administrative and financial sanctions for violations. Similar to its all LFIs, the CBUAE applies the principle of proportionality in its supervision and enforcement process, whereby small RHP may demonstrate to the CBUAE that the

[4] The CBUAE will issue Guidance for LFIs providing services to Cash Intensive Businesses.

objectives are met without necessarily addressing all of the specifics cited in the legal and regulatory framework in the UAE.

4.1 Permitted and non-permitted services by RHP

RHP are only permitted to provide well-defined services, which include non-commercial personal remittances and money transfer services to support commercial operations (such as trade transactions with jurisdictional corridors serviced by the hawala community).

RHP are not permitted to engage in any of the following transactions:

- Take deposits, exchange currencies or sell and purchase travellers' cheques;
- Provide any financial services other than money transfers (e.g. exchange of virtual assets/cryptocurrencies, loans, purchase of debts); or
- Execute transactions involving or on behalf of any other hawala provider in the UAE (as they are required by Circular No. 24/2019 to manage their business personally and never assign such task to another person, also known as "*nesting*"). This excludes the agents of the RHP in a foreign country (see also Part II section 3.3.5 below).

Part II: Guidance for RHP

1 Sanctions Obligations and Freezing Without Delay

Targeted Financial Sanctions (TFS) are legal restrictions on financial activity imposed by the United Nations Security Council (UNSC) or the UAE. An individual or legal person subject to TFS cannot send or receive money, or engage in any other kind of financial activity, without specific permission from the government of the UAE. The names of individuals or legal persons that are subject to TFS are included in lists published by the UN and the UAE (also known as "*listed persons*" or "*sanctioned persons*.")

RHP 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, the "*Guidance on TFS for FIs and Designated Non-Financial Business and Professions (DNFBPs)"* issued by the Executive Office of the Committee for Goods & Material Subject to Import and Export Control ("Executive Office"), the "*Guidance for LFIs on the implementation of TFS*" issued by the CBUAE, the CBUAE Notice No. 3895/2021, and any of their amendments or updates thereof.[5] RHP should be aware that it is a crime in the UAE to provide funds or financial services, including money transmissions services, to a person subject to TFS. This means that if a person is subject to TFS, the RHP cannot do any of the following:

- Send that person money on behalf of a customer, no matter where in the world they are;
- Provide that person with money that another person has sent them; or

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

- Carry out a transaction of any kind for that person.

Appropriate implementation of TFS has four key steps, which RHP must follow to ensure they are compliant:

1. **Maintain awareness of UNSC and UAE sanctions lists, and rapidly become informed of changes to these lists.**

RHP should rely on the official website of the UNSC for the most updated UN Consolidated List:

- https://www.un.org/securitycouncil/content/un-sc-consolidated-list

RHP should rely on the official website of the Executive Office to obtain the most recent publication of the UAE sanctions List (Local Terrorist List) List issued by the UAE Cabinet:

- https://www.uaeiec.gov.ae/en-us/un-page
- https://www.uaeiec.gov.ae/ar-ae/un-page

In addition, under Article 21 of Cabinet Decision 74, RHP must register on the Executive Office's website in order to receive automated email notifications with updated and timely information about the listing and de-listing of individuals or entities in the Local Terrorist List and in the UN Consolidated List.

2. **Check the names of customers against the lists of sanctioned persons.**

Every time an RHP carries out a transaction, it must check before it sends or receives any money to make sure its customer, counterparty, or anyone else involved in the transaction is not listed on the UN or UAE sanctions lists. This process is known as 'screening process.' The RHP must screen the customer and the person to or from whom the customer is sending or receiving money. Where the customer is a legal person, it must screen the customer's beneficial owners (see section 3.3.3 below) and senior managing official. The RHP must also screen its counterparty who is executing the transaction at the other end. The result of the screening process can have the following results:

- A "confirmed match"; i.e. a customer or a customer's counterparty has the same full name as a sanctioned person; or
- A "potential match"; i.e. a customer or a customer's counterparty has a similar or partially matching name as a sanctioned person; in those cases, the RHP should use additional information, such as the person's date of birth, address, and nationality, to distinguish the two persons.

In addition, every time there is a change to the sanctions lists, the RHP must compare the newly listed persons against its list of past customers. If an RHP finds that it previously carried out a transaction involving a person who was not listed at the time but is now listed, it has not done anything wrong. But it must report the transaction so that the authorities are aware (see step 4 below).

3. **Immediately freeze any funds in the possession or under the control of the RHP that may belong to a listed person and cancel (where possible) any transactions involving a listed person.**

When a "confirmed match" is found through the screening process, RHP must immediately, without delay and without prior notice, freeze all funds.

i. "Freeze all funds" means that you must hold the funds. You cannot send them or give them to anyone except to a UAE authority. You cannot return them to the person who gave them to you. If the funds are cash, you should place the funds in a safe place, separate from other funds, until the authorities can collect them. If the funds are held in a financial institution, such as a bank, you should notify the financial institution, who will place them in a special account. If an RHP has recently completed a transaction that involves a listed person, the RHP should notify its counterparty so that they can freeze the funds at the other end if possible. It must keep records of the information that it used to confirm this.
ii. "Without delay" means within 24 hours of the listing decision being issued by the UNSC, the Sanctions Committee or the UAE Cabinet, as the case may be. This means that you must take active efforts to become aware of changes to the sanctions lists by registering on the Executive Office's website in order to receive automated email notifications, and that once a change has been made, you must immediately put it into effect by refusing to carry out any transactions for or with a listed person.
iii. "Without prior notice" means that you must not tell the customer, or the person whose funds are being frozen, what the RHP is going to do.

When a "potential match" is found through the screening process, the RHP must suspend without delay any transaction and refrain from offering any funds or services. It must keep records of the information that it used to confirm this.

4. Report any listed persons and the actions the RHP has taken to the appropriate authorities

With regards to LFIs obligation for TFS reporting, the CBUAE in coordination with the Executive Office, has established a unified mechanism to report TFS obligations utilizing the UAE Financial Intelligence Unit's (FIU) online reporting platform (goAML).

In case of any "confirmed match" to a listing of names of individuals or legal persons to the Local Terrorist List and the UN Consolidated List, the RHP are required to report any freezing measures, prohibition to provide funds or services or any attempted transactions via the goAML platform within two business days by selecting the Fund Freeze Report (FFR). The RHP must also ensure all the necessary information and documents are submitted.

In case of any "potential match" to a listing of names of individuals or legal persons to the Local Terrorist List or UN Consolidated List, the RHP are required to report the potential match via the goAML Platform by selecting the Partial Name Match Report (PMNR). The RHP must also ensure all the necessary information and documents are submitted. In addition, the RHP must uphold suspension measures related to the "potential match" until further instructions are received via the goAML Platform on whether to cancel the suspension or implement freezing measures.

The TFS related reports (FFR or PMNR) submitted via the goAML Platform will be received simultaneously by the CBUAE and the Executive Office. RHP should also consult the CBUAE's[6] and the Executive Office's[7] websites respectively as updated from time to time.

[6] Available at: https://www.centralbank.ae/en/cbuae-amlcft
[7] Available at: https://www.uaeiec.gov.ae/en-us/un-page

2 Registration and other Requirements

2.1 Registration

Under Article 2 of Circular No. 24/2019, **a resident natural person or legal person may not carry on Hawala Activity in the UAE unless the applicant holds a Hawala Provider Certificate issued by the CBUAE** and registered in the CBUAE Hawala Providers Register. Any resident natural person or legal person may apply for registration and obtain a Hawala Provider Certificate from the CBUAE. The applicant should not be of UAE nationality, should be legally competent, and officially residing in the UAE. The said application shall be made on the CBUAE's prescribed forms on the CBUAE's website.[8]

2.2 CBUAE Notification of Approval/Rejection

Under Article 3 of Circular No. 24/2019, the CBUAE may agree or decline an application for a Hawala Provider Certificate. In case of approval, the CBUAE shall issue a Hawala Provider Certificate valid for one year, renewable for similar periods. The CBUAE shall notify the applicant in writing, and may include in the Hawala Provider Certificate whatever terms and conditions it deems appropriate. In case of rejection, the CBUAE shall notify the applicant in writing indicating reasons for rejection.

2.3 Re-Registration

Under Articles 2 and 4 of Circular No. 24/2019, RHP should submit to the CBUAE an application for renewal of the Hawala Provider Certificate within a period of not less than two months from the date of expiry of the original certificate or any renewals thereof. The said application should be made on the CBUAE's prescribed form titled "*Application to Re-register Hawala Providers*" on the CBUAE's website.

2.4 Requirements for Trade License, Security and Reporting Systems

As per Article 2 of Circular No. 24/2019 and the respective application requirements, RHP must complete the following requirements within 90 days from the date mentioned in the final registration certificate as well as submit proof of completion to the Licensing Division of the CBUAE:

- Add Hawala Activity to the commercial trade license.
- Install security systems; i.e. CCTV and police connections.
- Register in the relevant Services Access Control Manager (SACM) and subsequently to the UAE FIU's goAML portal by following the steps in the registration guides issued by the FIU previously sent to RHP. Registration on SACM is a prerequisite for goAML registration;
- Register in the relevant SACM and subsequently to the CBUAE's Remittance Reporting System (RRS) for the daily reporting and Integrated Regulatory Reporting System (IRR) for the quarterly reporting (see Part II section 4 below). Registration in SACM is a prerequisite for RRS & IRR registration. In order to register in SACM, RHP will be required to provide the following information to the CBUAE via e-mail on hawala@cbuae.gov.ae:

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

- Trade name of the RHP;
- First and last name of the user;
- Emirates ID number and copy of Emirates ID;
- Email address; and
- Mobile phone number.

- RHP should register for the Integrated Enquiries Management System (IEMS) by referring to the IEMS User Guide available at the relevant link in FIU's website.[9]

Failure to submit the above within the specified period may result in a registration certificate withdrawal.

2.5 Requirement for a Bank Account

As per Article 2 of Circular No. 24/2019 the RHP must maintain an account with a bank operating in the UAE to be used for settlement and provide the CBUAE with details of such account. In addition, they should inform their account manager at the bank of their intention to use the account to carry out Hawala Activity.

3 AML/CFT Program

As per Articles 4, 20, 21 and 26 of the AML-CFT Decision, RHP are required to establish and maintain effective AML/CFT compliance programs designed to prevent them from being misused to facilitate money laundering or terrorist financing (ML/TF). The program must be risk-based and appropriate to the risk of the RHP, taking into consideration its:

- Size;
- Volume of transactions;
- Types of remittances offered (personal only or personal and commercial);
- Complexity;
- The nature and volume of its Hawala Activity;
- The nature of its customer base; and
- The geographic areas in which it operates.

This means that where an RHP engages in higher-risk activities (as discussed below in section 3.2), or does a higher volume of business, it must have a more sophisticated AML/CFT program and employ more intensive measures to manage this risk. The section that follows discusses the **mandatory minimum elements** of an AML/CFT program under the legal and regulatory framework in the UAE as well as ways that RHP can make adjustments to respond to their risk. It is divided into four parts, as follows:

1. **The AML/CFT Program and the Compliance Officer**. This part discusses the content of the AML/CFT program and how it should be implemented by the RHP.
2. **Understanding Risks.** This section discusses how to identify the RHP's ML/TF risks so that the RHP can build an appropriate AML/CFT program.
3. **Customer Due Diligence**. This section discusses the mandatory procedures for identifying and understanding the RHP's customers and counterparties.

[9] Available at: https://www.uaefiu.gov.ae.

4. **Record Keeping**. This section discusses the records of activity that the RHP must maintain and provide to law enforcement authorities and counterparties.

3.1 The AML/CFT Program and the Compliance Officer

As per Article 21 of the AML-CFT Decision, each RHP must have a specific person, the Compliance Officer, who is responsible for day-to-day compliance with the legal and regulatory framework in the UAE and the management of the AML/CFT program. This person must be an employee, manager, or owner of the RHP. **In large RHP**, with multiple employees and substantial revenues from Hawala Activity, the CBUAE expects that the Compliance Officer will be a full-time position without any other responsibilities for managing the business. **In small RHP**, however, the CBUAE recognizes that the Compliance Officer is likely to have other responsibilities beyond management of the compliance program. If the RHP is owned and operated by a single person, that person will be the Compliance Officer.

The Compliance Officer is responsible for the following:

- Ensure full compliance with the legal and regulatory framework in the UAE and this Guidance.
- Making sure that other employees of the RHP (where relevant) comply with the legal and regulatory framework in the UAE and this Guidance, and abide by the RHP's own policies and procedures; and
- Implementing the compliance program elements described in this Guidance, including conducting the risk assessment.

The RHP's AML/CFT compliance program must include all the measures discussed in the following sections as well as the following components:

- **Provide education and training to appropriate personnel.** RHP employees who participate in Hawala Activity must be trained to understand how to comply with the legal and regulatory framework in the UAE and this Guidance, and abide by the RHP's policies and procedures. It is not acceptable for an untrained employee to have responsibility for collecting or disbursing customer funds and initiating transactions.
- **Conduct a periodic audit of the AML/CFT program.** RHP are required to arrange for a regular independent audit of their program by hiring an external qualified independent auditor approved by the CBUAE. **Small RHP** should be audited once every two or three years, while **large RHP** once every year. It is important to note that the audit must be independent; i.e. an RHP may not audit itself.

3.2 Understanding Risks

According to Article 16 of the AML-CFT Law and Article 4 of the AML-CFT Decision, RHP must identify, assess and understand the ML/TF risks to which they are exposed, and how they may be affected by those risks, in order to determine the nature and extent of AML/CFT resources necessary to mitigate and manage those risks. The sophistication of an RHP's risk assessment process depends on the RHP's size and operations. A **large RHP** is expected to produce an extensive risk assessment that complies fully with the standards outlined in the *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 79/2019 dated 27/06/2019) and any amendments or updates thereof. This assessment may be done by an external consultant, but the RHP

retains ultimate responsibility for its content and its compliance with the standard set in the Guidelines. The CBUAE recognizes, however, that a **small RHP** has limited services and resources. RHP of this type can follow the risk assessment process discussed below. All RHP must document their risk assessment, even if it is in the form of notes, to demonstrate that they have thoughtfully completed this process. They must be able to understand their findings and explain them if called upon to the CBUAE.

The Compliance Officer should begin the risk assessment process by carefully reading and understanding Parts I and II of this Guidance, which contain essential information about the risks faced by an RHP. The Compliance Officer should then consider the RHP's risk in the following risk categories. The discussion below does not cover every factor that increases or decreases risk and RHP should consider any other factors based on their knowledge and experience.

1. **Customer Risk.** This is the risk that your customers may be involved in ML/TF. By receiving money from a customer who is involved in illegal activities, the RHP itself can unwittingly become involved in those activities. Some examples of questions that RHP can use to assess customer risk include:
    a. *Are my customers mostly individuals, or do I have many customers that are legal persons?* When you provide services to a company, you don't always know who you're really dealing with. So having many legal person customers may increase your risk.
    b. *Are my customers only sending remittances to family, or are they engaging in business?* Business activities are generally considered to be higher risk for ML/TF because amounts are higher and it's harder for the RHP to understand the true purpose of the transaction.
2. **Geographic Risk.** Some countries are high risk for illicit activity, whether because they have a high volume of crime and terrorism, or because their financial sector doesn't have controls to prevent the movement of illicit funds. If an RHP operates in those countries, either because it has agents there or because it frequently sends or receives money there, then it is exposed to that risk. Questions an RHP can ask to assess its geographic risk include:
    a. *Do I regularly do business in or with countries that have an ongoing insurgency? Where terrorist attacks are frequent?* These countries will be very high risk.
    b. *Do I regularly do business in or with countries listed on the FATF list of monitored jurisdictions?*[10]
3. **Products and Services Risk.** RHP are permitted to offer only limited products and services (see Part I section 4.1 above). Within the group of permitted products, transfers connected to commercial activity are generally considered to be higher risk than those connected to personal remittances.
4. **Delivery Channel Risk.** The way an RHP delivers its products and services will also impact its risk, because some delivery channels make it difficult to understand and observe the customer. For example, if an RHP accepts orders for remittances via text message or phone call, or allows customers to initiate a transaction by giving money to an associate, who then delivers it to the RHP, this will make their activities higher risk.

[10] The FATF list can be found at https://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate).

Based on the considerations above, RHP should give themselves an overall score of Low, Medium, or High risk. **RHP should complete the risk assessment process at least once a year.** RHP should understand their risk assessment, its findings, and what it means for their business. They should consider their risk assessment when designing and implementing their AML/CFT program. Where they assess themselves as higher risk, they should take additional precautions.

3.3 Customer Due Diligence

Customer due diligence ("CDD") is the process by which an RHP identifies and understands its customer. CDD is required by Article 5 of the AML-CFT Decision and is essential to protecting the RHP from abuse, and to deterring and detecting ML/TF schemes. In specific cases outlined below, and whenever the RHP believes that higher risks are present, the RHP must perform Enhanced Due Diligence ("EDD"). EDD involves more intensive measures to discover information about the customer.

The RHP must perform Customer Identification Diligence ("CID"), CDD or EDD prior to conducting each and every transaction, even if the customer is a repeat customer (see sections 3.3.1 to 3.3.4 below for their details). **An RHP must not conduct a transaction if the appropriate diligence has not been performed or completed.**

When to Use CID, CDD and EDD	
Transaction	**What is Required**
A natural person sends or receives a transfer between AED 1 and AED 3,499	CID, unless higher risks are present, in which case CDD & EDD as well.
A natural person sends or receives a transfer of between AED 3,500 to AED.54,999	CDD, unless higher risks are present, in which case EDD as well.
A natural person sends or receives a transfer of AED 55,000 or greater.	CDD and EDD
A natural person from a high-risk jurisdiction sends or receives a transfer of any value.	CDD and EDD
A natural person who is a politically exposed person sends or receives a transfer of any value.	CDD and EDD
A legal person sends or receives a transfer of any value.	CDD and EDD

3.3.1 Customer Identification Diligence

The CID process must be applied for a natural person who sends or receives a transfer between AED 1 and AED 3,499. The CID process is the verification of the original identification documents of the customer who is a natural person and the systematic recording of basic customer information in the point of sale system without the need to retain copies of the identification documents. The customer's full name, address, mobile number, nationality, date of birth, ID type (Emirates ID, or passport number when Emirates ID is not available) and ID number must be recorded in the point of sale system and printed on receipts.

3.3.2 Customer Due Diligence for Natural Persons

Article 4 of Circular No. 24/2019 requires RHP to identify and verify the identity of their customers, including remitters and beneficiaries, by using Emirates ID, or passport when Emirates ID is not available. **RHP must collect at least the following information for each customer:**

- Name,
- Emirates ID number or passport number when Emirates ID is not available;
- Date of birth and nationality;
- Address;
- Mobile number;
- Occupation; and
- The name of the person from whom the customer is receiving money, or the person to whom the customer is sending money and their country.

This information must be printed on customer receipts. RHP must record this information and store it in their files for five years. RHP must also take a clear photo or photocopy of the customer's identification document and retain it for five years.

The CDD process should also be applied when it appears that a natural person may be deliberately splitting up a larger transfer to evade the CDD requirement (for example by repeatedly once in a week transfer value below AED 3,500 per transaction).

Using this information, as discussed in Part II section 1 above on sanctions obligations, RHP should screen their customers, including the sender/beneficiary as appropriate, and the transaction against the UN Consolidated List and the Local UAE Terrorist List. Screening must be performed before carrying out any transaction for the customer. If there is a match, the RHP should carefully consider whether the other data collected (date of birth, country of birth) match the information available for the listed person in question. The RHP may continue with the transaction only if it is confident that its customer or the person on the other end of the transaction is not a listed person. In addition, if the RHP discovers that any party to the transaction is listed on the UN Consolidated List and the Local Terrorist List, it must not return the customer's funds or provide the customer with funds that have been sent to him, but must instead freeze the funds.

Furthemore, RHP should obtain a clear understanding of the intended purpose and nature of the transaction and ensure that it does not breach the permitted services by RHP listed in Part I section 4 above. RHP should consider whether it is consistent with what they know about the customer. Some examples of transactions that may require further investigation include:

- A customer who says he works as a labourer wishes to transfer a sum that is greater than the average yearly income for someone in his position.
- A customer visits the RHP on a regular basis and makes small or moderate-sized transfers, but the sum of the amounts he transfers over the course of the year is greater than the yearly income for someone in his position.
- A customer says that he has no occupation, but continues to make transfers or transfers a large sum.
- A customer who is from country A states that he is sending funds to a family member, but the beneficiary is located in country B.

- A customer from country A makes regular transfers to people he says are family members in that country, but they appear to live in different regions of country A and their relationship to the customer is not clear.

These transactions are not necessarily illicit, but they suggest that the RHP needs to collect additional information. For example, a customer may actually be acting on behalf of a business. In that case, the RHP's customer is actually the business, and it must perform CDD on the business as described in section 3.3.3 below. If the RHP has any additional concerns, it should follow the EDD procedures discussed in section 3.3.4 below.

RHP must cease and reject any transaction if they cannot collect any of the information required above, or if they cannot comply with any of the above requirements.

3.3.3 Customer Due Diligence for Legal Persons

When a legal person like a company uses an RHP to conduct a transaction, the RHP's customer is the company itself, not the individual representing the company. A legal person conducts a transaction when the funds involved belong to the legal person, and when the transaction is made as part of carrying out the legal person's business. If the customer is a legal person, it must be registered and based in the UAE to carry out transactions through a RHP. Legal persons such as companies, bodies corporate, foundations, partnerships, or associations, along with similar entities do not have bio-data like individuals and can transact under their own names while being controlled by other individuals. This means that they require specific CDD procedures. As per Articles 8 and 9 of the AML-CFT Decision **RHP must perform the following actions for a legal person customer:**

1. Collecting and recording the following information about the legal person customer:
    a. The legal person's name;
    b. The legal person's legal form (e.g., limited liability company);
    c. The address of the legal person's main office or headquarters;
    d. The legal person's trade license; and
    e. The name of the legal person's senior managing official.
2. Conducting CDD as described in section 3.3.2 above on the individual representing the customer (the individual who is directly ordering the transaction).
3. Determining that the representative is authorized to conduct the transaction via a valid authorization, such as the trade license and/or a letter from the legal person customer's management on its letterhead.
4. Identifying and verifying the identity of the customer's beneficial owners.
    a. Beneficial owners are the individuals who own and control the legal person. In many cases, the managing director or other similar top official will also be the beneficial owner, but not always.
    b. RHP must identify every individual who owns 25% or more of the legal person customer. They must collect their names, and then perform CDD on them as required by section 3.3.2 above.
    c. RHP can collect the names of beneficial owners, and thus determine who to perform CDD on, by asking the customer's representative. If they are concerned about the information provided by the representative, they should ask for documentation to prove ownership.

   d. If no individual owns 25% of the legal person customer, RHP must identify, and conduct CDD on the individual who is the customer's senior managing official.
   e. Beneficial owners cannot be other legal persons. If a legal person customer is owned by other legal persons, the RHP must understand their ownership as well until it identifies all individuals owning at least 25% of its customer.
5. Understanding the customer's ownership and control structure. The RHP must understand who owns the customer, who exercises control over it and how.
6. Understanding the nature of the customer business. The RHP must understand what sort of business the customer engages in and how the customer makes its money. If the customer's business doesn't make sense, or if the customer has no apparent business activities, that calls into question whether the funds involved in the transaction actually came from legitimate business activities.

- Conducting sanctions screening on all related parties. The RHP must at least screen the following names against sanctions lists:
   a. The name of the legal person customer;
   b. The name of the customer's representative;
   c. The name of the beneficial owner(s);
   d. The name of the customer's senior managing official; and
   e. The customer's address.

As with CDD for natural persons, RHP must take a clear, readable photo or photocopy of documents obtained from the customer during CDD, and must retain those documents for five years after the transaction.

3.3.4 Enhanced Due Diligence

Sometimes CDD alone as described above is not sufficient to fully understand a customer. In addition, for certain customers, an extra level of due diligence is required. In those cases, the RHP must perform EDD in the following circumstances:

1. The customer is a legal person. In these cases, the RHP must perform all the steps listed in section 3.3.3 above, plus additional due diligence as described here.
2. The customer is a natural person carrying out a transfer worth AED 55,000 or above. In those cases, the RHP must perform all the steps listed in section 3.3.2 above, plus additional due diligence as described in this section below.
3. The customer is a politically exposed person. During CDD, the RHP must collect information regarding the occupation of a natural person customer, and the beneficial owners of a legal person customer. If the customer, or the beneficial owners of a legal person customer, indicates that he or she is a government official with any government, the RHP must ask additional questions to understand that individual's rank and status. If the individual holds a high-ranking position in any government, then EDD is required for the customer. This is to make sure that the funds involved are not related to corruption or abuse of the customer's position.
4. The customer is from, or is sending a remittance to, a high-risk jurisdiction. As discussed in section 3.2 above, high-risk jurisdictions are those with a higher risk of ML/TF.

RHP should **consider** performing EDD when there are other high risks associated with the transaction, such as concerns about the customer's behaviour or about the source of the funds involved in the transaction.

When performing EDD, RHP must follow the following mandatory steps:

- Seek approval from the manager of the RHP to carry out the transaction. If the RHP is owned and operated by a single person, this step is not necessary.
- Collect additional information to understand the source of funds involved in the transaction and the customer's overall source of funds (i.e. source of wealth). For instance, the RHP may ask for a pay slip to verify the customer's income.
- Collect additional information about the customer's business. For example, if a transaction is linked to the sale of goods, the RHP may request to see the invoice.

3.3.5 Agent Due Diligence

RHP may use agents in a foreign country to carry out activity on their behalf in that foreign country. This generally entails the corresponding agent in the foreign country executing payments on instructions from the RHP, or the agent sending instructions to the RHP to execute payments domestically. It should be noted that **RHP are not permitted to use agents to carry out activity on their behalf in the UAE** (as they are required by Circular No. 24/2019 to manage their business personally and never assign such task to another person, also known as "*nesting*".)

RHP are exposed to risks when their agents engage in transactions that create risks for ML or TF. RHP must identify and assess the ML/TF risks they may be exposed to from the use of agents to provide activity on their behalf in a foreign country. RHP should ensure that they understand who their agents are, and that they are not breaching any applicable AML/CFT laws and regulations. In order to reduce their exposure to ML/TF risks, RHP are required to perform appropriate due diligence on their agents, to ensure they thoroughly know their agents and monitor their transactions to ensure that they are legitimate. **The required elements of due diligence on agents are as follows:**

- When entering into a business relationship with an agent, as a first step, the RHP should identify and verify the identity of the agent, using reliable, independent source documents, data or information.
- RHP should also identify and take reasonable measures to verify the identity of the beneficial owner(s) and understand the ownership and control structure of the agent, such that the RHP is satisfied that it knows the beneficial owner(s) and that the agent is not a shell bank.
- RHP should gather sufficient information to understand the purpose and intended nature of the business relationship, which includes understanding what types of customers the agent intends to service through the business relationship, how it will offer services, the transaction volume and value, and the extent to which any of these are assessed as high risk.
- RHP should also gather sufficient information and determine from publicly available information the reputation of the agent, including whether it has been subject to a ML/TF investigation or regulatory action. In addition, RHP should ensure that the agent has proper AML/CFT controls.
- RHP should conduct ongoing due diligence of the business relationship, including periodical reviews of the CDD information on the agent, and ongoing monitoring to detect any changes in the agents' activity pattern that may indicate unusual activity.

RHP should keep up-to-date agent lists and retain them for a period of five years. RHP must provide the CBUAE current lists of their agents and the countries in which they operate. In addition, RHP should make current lists of their agents available to the relevant authorities within the country in which they operate. RHP should ensure that their agents fully adhere to the procedures of record keeping as described in this Guidance and that they make those records available to the RHP immediately upon request.

3.4 Record Keeping

Under Article 16 of AML-CFT Law and Article 24 of the AML-CFT Decision, RHP, as remittance providers, have very important obligations relating to the records they maintain about the remittances they execute.

3.4.1 Record Keeping Related to Remittances

1. *Sending a Remittance*

When the RHP's customer is the person originating a transaction, the RHP must collect the following information through the CID and CDD process:

- The sending customer's name;
- His or her Emirates ID, or passport number when Emirates ID is not available;
- His or her date and nationality;
- His or her address;
- Mobile number;
- Occupation; and
- The name of the beneficiary of the transaction and the country it is sent to.

The RHP must assign the transaction a unique ID number that allows the RHP to quickly identify and track the transaction. The RHP must provide all of this information to the hawala provider at the other end of the transaction and keep the relevant record. **The RHP must not carry out the transaction if it has not supplied this information.**

2. *Receiving a Remittance*

When the RHP's customer is the person receiving the remittance, the RHP must conduct CDD on the beneficiary and make sure that its customer's information matches that of the beneficiary identified in the information provided by the Originating Hawala Provider and keep the relevant record. The information must include:

- The receiving customer's name;
- His or her Emirates ID, or passport number when Emirates ID is not available;
- His or her date and nationality;
- His or her address;
- Mobile number;
- Occupation; and
- The name of the sender of the transaction and the country it is sent from.

The RHP's partners and agents outside the UAE should comply with the requirements under "*Sending a Remittance*" above even though they are not subject to UAE laws. If a RHP receives a transaction order from a hawala provider outside the UAE that does not contain the information required

under "*Sending a Remittance*" above, it cannot perform required sanctions screening or identify whether the transaction is suspicious and needs to be reported to the FIU. Therefore, the RHP should require its agent or counterpart to provide the information listed before it releases the funds to the beneficiary.

3.4.2 Other Types of Record Keeping

According to the AML-CFT Law and the AML-CFT Decision, RHP must keep all records obtained through the CDD process; copies of personal identification documents provided during CDD; and copies of Suspicious Transaction Reports (STR) filed with the FIU. Under Article 4 of Circular No. 24/2019, RHP are required to have forms in which the customers fills in the necessary information to originate the transaction; RHP must retain these forms as well.

RHP must also maintain records of transactions. These records must be sufficiently detailed to allow authorities to reconstruct and understand the transaction. They must at least include the names of the sender and beneficiary, the date of the transaction, and the amount of the transaction, and be organized in such a way so that the RHP and authorities can easily find the records they need for a specific transaction.

RHP must make the records described here, or any other records, available to the competent authorities immediately upon request. All the records described in this section must be kept for at least five (5) years, from the date of completion of the transaction, or for longer if directed by the CBUAE or other authority.

4 Reporting Obligations

4.1 Daily Reporting

Under Article 4 of Circular No. 24/2019, RHP are required on a daily basis to upload electronically to the CBUAE, via its Remittance Reporting System ("RRS") and/or other applicable system, the data and details of all transfers, remitters and beneficiaries as per the forms prepared by the CBUAE for this purpose.

4.2 Quarterly Settlement Statements

Under Article 4 of Circular No. 24/2019, RHP should submit to the CBUAE statements of their settlement accounts on a quarterly basis along with other required forms, as well as provide the CBUAE with any data, information, or statistics it may require at any time and for any specific period.

4.3 Reporting Suspicious Transactions and registration to GoAML

RHP must monitor transactions that they carry out to identify those that may be suspicious and where a Suspicious Transaction Report ("STR"), or suspicious activity report ("SAR") or other report types may need to be filed with the FIU. Monitoring begins at the CDD stage, but does not end there. RHP must keep records of customer activity so that they can examine it to identify patterns over time that may be cause concern. RHP must take into account all information available, including regarding the originator and beneficiary(ies) of a transaction, in order to determine whether an STR is to be filed.

Situations in which it may be necessary to file an STR/ SAR include:

- A customer begins the CDD process, but cancels the transaction and leaves when he discovers the information that the RHP is required to collect.

- The RHP completes CDD on a customer, but still has doubts as to whether the transaction was legitimate or whether the customer's stated reason for the transaction was the true one.
- A customer carries out transactions larger than his stated income without providing a valid justification.
- A natural person customer regularly orders transactions just below the AED 55,000 threshold for when EDD is required (i.e. either tied to the threshold or if there are other risk factors that may trigger EDD).
- Multiple customers send money to, or receive money from, the same person, and there is no clear connection between the customers.
- The RHP suspects that a customer is carrying out transactions that are disallowed under Part I, section 4.1 of this guidance.

Under Article 15 of the AML-CFT Law and Article 17 of the AML-CFT Decision, if the RHP suspects that a transaction, attempted transaction, activity, or funds (including agents' transactions), 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, they must submit an STR, SAR or other report types to the FIU using the "goAML" portal. RHP must submit this report without delay, meaning as soon as reasonably possible after the transaction takes place or their suspicions develop. All RHP must register with the goAML portal so that they can easily file these reports.

Reporting a suspicious transaction is not an admission of guilt or wrongdoing. STRs filed by RHP help law enforcement authorities identify and track potential criminal behaviour. As long as the RHP complies with the procedures in this guidance document, it will not generally be held responsible for a transaction that turns out to have been involved in a crime. But a failure to report a transaction that an RHP should know to be suspicious can result in penalties.

For more detail and information, please refer to the "*CBUAE Guidance for Licensed Financial Institutions on Suspicious Transaction Reporting*."

5 Penalties

Under Article 7 of Circular No. 24/2019, violation of any provision may be subject to supervisory action as deemed appropriate by the CBUAE. In addition, without prejudice to other sanctions stated in other laws in the UAE, the CBUAE may impose administrative and financial sanctions and penalties in accordance with the Decretal Federal Law No. (14) of 2018 Regarding the Central Bank & Organization of Financial Institutions and Activities and the CBUAE Regulations issued in implementation thereof.

Part III: Guidance for LFIs

1 Understanding Risks

Please refer to Part I, Section 3 for a description of the risks of Hawala Activity.

The Circular No. 24/2019 requires that RHP must maintain an account with a bank operating in the UAE to be used for settlement and provide the CBUAE with details of such account. **The CBUAE expects LFIs to accept RHP customers**, but LFIs must manage the risk that these transactions create through the use of appropriate controls (see Part III, section 2 below). **LFIs must not accept as customers *unregistered* hawala providers based in the UAE, and must immediately report an STR to the FIU, inform CBUAE when they are detected, and closely monitor the relationship.** Please see Part III, sections 2.2 and 2.3 below for guidance on detecting *unregistered* MVTS.

2 Mitigating Risks

The sections below elaborate on how LFIs can apply specific preventive measures to identify, manage, and mitigate the risks associated with hawala providers customers. These are not exhaustive and LFIs should consult the legal and regulatory framework in force in the UAE for the measures to be taken. The controls mentioned below should be **at the minimum** integrated into the LFI's larger AML/CFT compliance program, and supported with appropriate governance and training.

2.1 Risk-Based Approach

LFIs should take a risk-based approach to the preventive measures they put in place for all customers, including hawala providers. **The risk-based approach has three principal components:**

2.1.1 Conducting an enterprise risk assessment

As required by Article 4.1 of the AML-CFT Decision, the enterprise risk assessment should reflect the presence of higher-risk customers, including hawala providers, in an LFI's customer base. These assessments should in turn be reflected in the LFI's inherent risk rating. In addition, the LFI's controls risk assessment should take into consideration the strength of the controls that the LFI has in place to mitigate the risks posed by its hawala providers customers, including the preventive measures discussed below.

2.1.2 Identifying and assessing the risks associated with specific customers

The LFI should assess the risk of each customer to identify those that require EDD and to support its entity risk assessment. As discussed in Part I section 3 above, the regulatory environment and illicit finance risks in the jurisdictions in which they do business, the products and services they provide and its customer base, are critical determinants of a hawala provider's inherent risk. In assessing the risks of a hawala provider customer, LFIs should consider:

i. **Controls Risk:** LFIs should seek to understand the regulatory requirements in place for the customer, as well as how well they are enforced. The regulatory requirements placed on hawala providers vary markedly across jurisdictions.

ii. **Geographic Risk:** The risks associated with the jurisdictions in which the provider lives (for individuals) or is registered/established (for legal persons) and where it operates, including the jurisdictions where its main counterparties are based and where it has subsidiaries.

iii. **Product, Service, and Delivery Channel Risk:** LFIs should assess risk in this category on two dimensions:

   a. The products and services that the hawala provider offers to its customers, and

   b. The delivery channels through which it offers these products and services.

   Products, services, and delivery channels that promote the rapid, anonymous transfer of high values are particularly attractive to illicit actors.

iv. **Customer Risks:** For hawala provider customers, customer risk can be assessed as the proportion of higher-risk customer types (e.g. politically exposed persons, legal persons, and customers from high-risk jurisdictions) within the provider's customer base.

Questions that an LFI may ask to determine the risk profile of a hawala provider customer include, but are not limited to:

- *Where is the provider incorporated? Where does it operate? Are these high-risk jurisdictions?*
- *What products and services does the provider offer its customers?*
- *What volume of transactions does the provider carry out?*
- *What customer base does the provider serve?*
- *What is the regulatory environment in the jurisdiction(s) where the provider is incorporated/has operations?*
- *Is there an authority that actively enforces the requirements?*
- *Does the provider perform appropriate CDD, transaction monitoring, record keeping, and sanctions screening?*
- *Does the provider intend to use its account to execute transactions on behalf of its customers?*

In addition to risk rating hawala providers, LFIs should also consider the risks of specific transactions, especially high-value transactions, those involving high-risk jurisdictions, and those that represent departures from a customer's standard or expected behaviour.

2.1.3 Applying EDD and other preventive measures

Where the LFI determines a customer to be higher-risk, Article 4.2(b) of the AML-CFT Decision requires that the LFI apply EDD. Specific EDD steps are also required for hawala providers customers that are politically exposed persons, or are owned or controlled by a politically exposed person, or are based in a higher-risk jurisdiction.

2.2 Customer Due Diligence and Enhanced Due Diligence

The goal of the CDD process is to ensure that LFIs understand who their customer is and the purpose for which the customer will use the LFI's services**. Where an LFI cannot satisfy itself that it understands a customer, then it must not accept the customer. If there is an existing business relationship, the LFI should not continue it.** LFIs should also consider filing an STR, SAR or other report types to the FIU as discussed in section 2.3.2 below. This guidance is not an exhaustive list of LFIs' CDD obligations and LFIs should consult the legal and regulatory framework in force in the UAE for the measures to be taken.

2.2.1 Customer Identification and verification

Under Article 8 of AML-CFT Decision, LFIs are required to identify and verify the identity of all customers. Please see also the *AML/CFT Guidelines for Financial Institutions* for full information on customer identification. In particular, when verifying the Emirates ID card, LFIs must use the online validation gateway of the Federal Authority for Identity & Citizenship and keep a copy of the Emirates ID and its digital verification.

Hawala providers based in the UAE are required to have an active registration certificate issued by the CBUAE and a commercial trade license that includes Hawala Activity. In particular, when opening any accounts for hawala providers, LFIs must physically check the original hawala provider registration certificate issued by the CBUAE and keep a copy thereof. LFIs should not form business relationships or conduct transactions with hawala providers without an active registration certificate issued by the CBUAE (*unregistered* hawala providers). In addition, if an LFI determines that a customer or prospective customer has materially misrepresented itself or its business, it must not accept the customer, must exit the relationship if one has been established, should add the customer, its beneficial owners, directors and managers to its internal watchlists, and should file an STR with the FIU*.*

2.2.2 Beneficial Owner Identification

Where the hawala provider customers is a legal person, please consult the CBUAE's *Guidance for LFIs providing services to Legal Persons and Arrangements* for details on the identification of beneficial owners.[11]

2.2.3 Customer's Business and Business Relationship

For all customer types, LFIs are required to understand the purpose for which the account or other financial services will be used, and the nature of the customer's business. This element of CDD will have important implications for the customer risk rating. This is particularly true of the purpose of the account, which will likely be an essential determinant of risk for hawala provider customers. It is critical that LFIs have processes and controls in place to ensure that they are able to identify hawala customers. LFIs must ensure that they fully understand their customers' source of funds and the business in which they are engaged. In addition to interviewing the customer, requesting financial records, and reviewing invoices, LFIs should also search company databases and consider visiting the customer's business premises.

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

Underground hawala providers often try to evade detection by creating new companies and/or frequently switching to new financial institutions. In addition, even those that operate legally, may seek to misrepresent the purpose of the relationship in order to evade scrutiny and controls imposed by the LFI. It can be particularly difficult for an LFI to establish the bona fides and business activities of a newly established company, which is likely to not have any customers or inventory, especially when that company's line of business (e.g. import/export) is vague. LFIs should screen the names of new customer's beneficial owners, directors, and managers against its internal watchlists of customers previously exited by the LFI.

When a customer provides information indicating it is a hawala provider, LFIs must collect sufficient information during the CDD process to understand the full scope of the customer's business, including not only its provision of hawala services but also any other business activities in which the customer engages. LFIs should pay particular attention to the jurisdictions with which their hawala provider customers does business, and must understand whether their customer offers financial services to other hawala providers (e.g. participates in clearing networks or makes transfers on behalf of the customers of another provider who lacks a network in certain jurisdictions). Furthermore, LFIs must fully understand the intended use of the account and the expected activity on the account, to the extent that it can generally predict activity on the account and identify activity that does not fit the profile. This may be many small cash deposits followed by large cross-border transfers or volume of activity that does not fit the customer's business. They must also understand whether the hawala provider may be using the LFI's accounts to conduct business and to move funds on behalf of customers while attempting to conceal this activity from the LFI. Section 2.3.1 contains red flags for concealed activity.

2.2.4 Ongoing Monitoring

All customers must be subject to ongoing monitoring throughout the business relationship to ensure that transactions are reasonable, and legitimate. Ongoing monitoring is particularly important in the context of business relationships with hawala providers, where the risks these relationships create for the LFI can change significantly based on the hawala provider's business activities. LFIs are required to ensure that the CDD information they hold on all customers is accurate, complete, and up-to-date. LFIs should update CDD for all customers on a risk-based schedule, with CDD on higher-risk customers being updated more frequently. EDD on all customers should involve more frequent CDD updates.

In addition to a review of the customer's CDD file, the LFI should also review the customer's transactions to determine whether they continue to fit the customer's profile and business, and are consistent with the business the customer expected to engage in when the business relationship was established. This type of transaction review is distinct from the ongoing transaction monitoring discussed in 2.3.1 below. The purpose of the review is to complement ongoing transaction monitoring by identifying behaviours, trends, or patterns that are not necessarily subject to transaction monitoring rules. For example:

- Company M, a hawala provider, opens an account with Bank B, an LFI. At onboarding, Company M tells Bank B that it operates as a money transfer service to Country X. A year after the account is opened, Bank B conducts a scheduled CDD review and discovers that, six months after onboarding, Company M began to make and receive periodic transfers to and from Country Y. Bank B makes inquiries and discovers that Company M is now providing money transfer services to Country Y as well. Bank B decides to put a restriction on the account requiring prior authorization to make transfers beyond Country X and Country Y, requires Company M to sign a warrant that it

will inform Bank B in advance of any future changes to its business model, and raises the customer risk-rating.

When customers are higher risk, including hawala provider customers, monitoring should be more frequent, intensive, and intrusive. LFIs should review the CDD files of higher risk customers on a frequent basis, such as twice a year. The methods LFIs use to review the account should also be more intense and should not rely solely on information supplied for the customer. For example, LFIs should consider:

- Reviewing all transactions on the account, rather than a sample of transactions;
- Conducting site visits at the customer's premises and requesting a meeting with the customer;
- Conducting searches of public databases, including news and government databases in order to independently identify material changes in a customer's ownership or business activities. Such searches should include adverse media searches of public records and databases, using relevant key words, including but not limited to, allegation, fraud, corruption, laundering.

2.3 Transaction Monitoring and STR Reporting

2.3.1 Transaction Monitoring

Where possible, transaction monitoring systems used to monitor activity in the accounts of the RHP should also be equipped to identify breaches of the permitted services by RHP listed in Part I section 4.1. The transaction monitoring system used by LFIs should also be equipped to identify RHP that are using the LFI's accounts to conduct their business and to move funds on behalf of customers while attempting to conceal this activity from the LFI. Red flags for concealed activity appear below. If an LFI's automated transaction monitoring system is not capable of alerting on these red flags, LFIs should have in place manual monitoring, such as management information systems that are capable of doing so. Frequent deposits by multiple individuals into a single bank account, followed by international wire transfers and /or international withdrawals through ATMs.

- Money being transferred at regular intervals to international locations known to be clearing houses for remittances.
- An account being used as a temporary repository with the funds quickly transferred.
- Usage of third-party accounts to disguise and to avoid detection by authorities.
- Wire transfers frequently sent by traders to foreign countries that do not seem to have any business connection to the destination countries.
- Business accounts used to receive or disburse large sums of money but show virtually no reasonable business-related activities such as payment of payrolls, invoices etc.
- Frequent deposits of third-party checks and money orders into business or personal accounts.
- Frequent international wire transfers from bank accounts that appear inconsistent with stated business activities.
- Sudden change in pattern of financial transactions from low value international fund transfers to large value transfers.

2.3.2 STR Reporting

As required by Article 15 of AML-CFT Law and Article 17 of AML-CFT Decision, LFIs must file an STR, or SAR or other report types with the FIU when they have 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. **STR filing is not simply a legal obligation; it is a critical element of the UAE's effort to combat financial crime and protect the integrity of its financial system.** STR filings are essential to assist concerned UAE authorities, such as law enforcement, in detecting criminal actors and preventing the flow of illicit funds through the UAE financial system.

In addition to the requirement to file an STR when an LFI suspects that a transaction or funds are linked to a crime, LFIs should consider filing an STR in the following situations:

- A potential customer decides against opening an account or purchasing other financial services after learning about the LFI's CDD requirements;
- A current customer cannot provide required information about its business or its beneficial owners;
- A customer cannot adequately explain transactions, provide supporting documents such as invoices, or provide satisfactory information about its counterparty;
- The LFI is not confident, after completing CDD procedures, that it has in fact identified the individuals owning or controlling the customer. In such cases, the LFI should not establish the business relationship, or continue an existing business relationship; or
- If the LFI believes that a customer may be acting as an unregistered hawaladar.

Please see also the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting* for further information.

2.4 Governance and Training

The specific preventive measures mentioned above must take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces. The core of an effective risk-based program is an appropriately experienced AML/CFT compliance officer who understands the LFI's risks and obligations and who has the resources and autonomy necessary to ensure that the LFI's program is effective. As with all risks to which the LFI is exposed, the AML/CFT training program must ensure that employees are aware of the risks of hawala provider customers, familiar with the obligations of the LFI, and equipped to apply appropriate risk-based controls. Training should be tailored and customized to the LFI's risk and the nature of its operations. For example, an LFI that has a large number of hawala provider customers should offer training that includes an in-depth discussion of risk factors and red flags related to such customers.

Annex 1. Synopsis of the Guidance

PART I: REGISTERED HAWALA PROVIDERS AND LICENSED FINANCIAL INSTITUTIONS		
Introduction	Purpose	The purpose of this Guidance is to assist the understanding and effective performance by the Registered Hawala Providers and other Licensed Financial Institutions (LFIs) of their statutory obligations under the legal and regulatory framework in force in the UAE.
	Applicability	This Guidance applies to all natural and legal persons which are licensed and/or supervised by the CBUAE in the following categories: Registered Hawala Providers ("RHP"), National banks, branches of foreign banks, and Exchange houses.
	Legal Basis	This Guidance builds upon the provisions of UAE laws and regulations, including the AML-CFT Law, the AML-CFT Decision, the Cabinet Decision 74 of 2020 and the Registered Hawala Providers Regulation issued by the CBUAE ("Circular No. 24/2019").
Overview of Hawala activity	Hawala is an activity based on trust and was established to avoid high charges by people who cannot afford them, the ability to reach beneficiaries in remote places quickly where banks do not operate, and the existence of strict currency controls in some countries. While hawala providers, also known as hawaladars, often use banking channels to settle between them, what makes them distinct from other money transmitters is their use of other settlement methods, including trade, cash, and long-term net settlement.	
Global risks of Hawala Activity	Hawaladars' business model is built around satisfying customers' needs to move money rapidly across borders, a service that may also be misused by criminals as it is to individuals seeking to conduct legitimate personal remittances. The risk of a hawala provider is influenced by the regulatory environment and illicit finance risks in the jurisdictions in which they do business, the products and services they provide, and their customer base.	
Regulation in the UAE	The CBUAE permits legitimate Hawala Activity as an important element of its continuous efforts to support financial inclusion and bring the unbanked population into the regulated financial system. To this end, Hawala is regulated by the Registered Hawala Providers Regulation issued by the CBUAE. All providers **carrying on Hawala Activity in the UAE must hold a Hawala Provider Certificate issued by the CBUAE**; it is not permitted to carry on Hawala Activity without being registered with the CBUAE. Registered Hawala Providers (RHP) are only permitted to provide well-defined services that include non-commercial personal remittances and money transfer services to support commercial operations. RHP are not permitted to engage in any of the following transactions: Take deposits, exchange currencies or sell and purchase travellers' cheques; Provide any financial services other than money transfers (e.g. exchange of virtual assets/cryptocurrencies, loans, purchase of debts); or Execute transactions involving or on behalf of any other hawala provider in the UAE. This excludes the agents of the RHP in a foreign country.	
PART II: GUIDANCE FOR REGISTERED HAWALA PROVIDERS		
Sanctions Obligations	Targeted Financial Sanctions (TFS) are legal restrictions on financial activity imposed by the United Nations Security Council (UNSC) or the UAE. RHP are required to fully comply with the obligation to implement all necessary measures without delay as described in the Cabinet Decision 74 of 2020, the "*Guidance on TFS for FIs and Designated Non-Financial Business and Professions (DNFBPs)*" issued by the Executive Office of the Committee for Goods & Material Subject to Import and Export Control, the CBUAE's *Guidance for LFIs on the implementation of TFS*, the CBUAE Notice No. 3895/2021, and any of their amendments or updates thereof. RHP should be aware that it is a crime in the UAE to provide funds or financial services, including money transmissions services, to a person subject to TFS. Appropriate implementation of TFS has four key steps, which RHP must follow to ensure they are compliant: 1. Maintain awareness of UNSC and UAE sanctions lists, and rapidly becoming informed of changes to these lists. 2. Check the names of customers against the lists of sanctioned persons. 3. Immediately freeze any funds in the possession or under the control of the RHP that may belong to a listed person, and cancelling (where possible) any transactions involving a listed person. 4. Report any listed persons and the actions the RHP has taken to the appropriate authorities (via the goAML Portal).	

PART II: GUIDANCE FOR REGISTERED HAWALA PROVIDERS (cont'd)		
Registration and other Requirements	Registration	A resident natural person or legal person may not carry on Hawala Activity in the UAE unless the applicant holds a Hawala Provider Certificate issued by the CBUAE and is registered in the CBUAE Hawala Providers Register.
	CBUAE Notification of Approval/Rejection	The CBUAE may agree or decline an application for a Hawala Provider Certificate and will notify the applicant in writing of its decision.
	Re-Registration	RHP should submit to the CBUAE an application for renewal of the Hawala Provider Certificate within a period not less than two months from the date of expiry of the original certificate or any renewals thereof.
	Requirements for Trade License, Security and Reporting Systems	RHP are required to complete the following requirements within 90 days from the date mentioned in the final registration certificate as well as submit proof of completion to the Licensing Division of the CBUAE: • Add Hawala Activity to the commercial trade license. • Install security systems i.e. CCTV and police connections. • Register o the UAE Financial Intelligence Unit's (FIU) goAML portal. • Register to the CBUAE's Systems for the daily and quarterly reporting. • RHP should register for the FIU's Integrated Enquiries Management System.
	Requirement for a Bank Account	RHP must maintain an account with a bank operating in the UAE to be used for settlement and provide the CBUAE with its details. In addition, they should inform their account manager at the bank of their intention to use the account to carry out Hawala Activity.
AML/CFT program	AML/CFT Program and Compliance Officer	RHP are required to establish and maintain effective AML/CFT compliance programs designed to prevent them from being misused to facilitate money laundering or terrorist financing. The program must be risk-based and appropriate to the risk of the RHP, taking into consideration its size, volume of transactions, types of remittances offered (personal only or personal and commercial), complexity, the nature and volume of its Hawala Activity, the nature of its customer base and the geographic areas in which it operates. Each RHP must have a specific person, the Compliance Officer, who is responsible for day-to-day compliance with the legal and regulatory framework in the UAE and the management of the AML/CFT program. This person must be an employee, manager, or owner of the RHP depending on the size of the RHP. They should also provide education and training to appropriate personnel and conduct a periodic audit of the AML/CFT program.
	Understanding Risks	The Compliance Officer should begin the risk assessment process by carefully reading and understanding Parts I and II of this Guidance, which contain essential information about the risks faced by an RHP and consider the customer, geographic, products and services, and delivery channel risks. RHP should complete this risk assessment process at least once a year. Where they assess themselves as higher risk, they should take additional precautions.

AML/CFT Program	Customer and Agent Due Diligence	Customer due diligence ("CDD") is the process by which an RHP identifies and understands its customer; it is required by law. The RHP must perform Customer Identification Diligence ("CID"), CDD or Enhanced Due Diligence ("EDD") prior to conducting each and every transaction, even if the customer is a repeat customer. An RHP must not conduct a transaction if the appropriate diligence has not been performed or completed depending on their nature as follows: • CID: When natural persons sends or receives a transfer between AED 1-3,499 and no higher risks are present. • CDD: In all other cases between AED 3,500-54,999. • EDD: When the customer is a natural person carrying out a transfer above ED 55,000, or when the customer is from/sending a remittance to a high-risk jurisdiction, or when the customer is a politically exposed person or a legal person, or when other higher risks are present. RHP may use agents in a foreign country to carry out activity on their behalf in that foreign country. RHP are not permitted to use agents to carry out activity on their behalf in the UAE (also known as "*nesting*"). RHP are required to perform appropriate due diligence on their agents and monitor their transactions to ensure that they are legitimate, keep up-to-date agent lists for a period of five years and provide them upon request to the CBUAE and/or to relevant authorities within the country in which they operate.
	Transaction Monitoring and Record Keeping	When an RHP's customer is originating a transaction, the RHP must collect and keep certain information for every transaction. When RHP's customer is receiving the remittance, they must in addition conduct CDD on the beneficiary and make sure that its customer's information matches that of the beneficiary identified in the information provided by the originating hawala provider. RHP must keep all records obtained through the CDD process and maintain records of all transactions for at least five years from the date of completion of the transaction or longer if directed by the CBUAE or any other authority.
Reporting Obligations	Daily Reporting	RHP must upload electronically to the CBUAE's reporting systems on a daily basis the data and details of all transfers, remitters and beneficiaries as per the forms prepared by the CBUAE for this purpose.
	Quarterly Settlement Statements	RHP must further submit to the CBUAE statements of their settlement accounts on a quarterly basis along with other required forms, as well as provide the CBUAE with any data, information, or statistics it may require.
	Reporting Suspicious Transactions to the FIU	If the RHP suspects that a transaction, attempted transaction, activity, or funds (including agents' transactions), 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, they must submit a Suspicious Transaction Report (STR), Suspicious Activity Report (SAR) or other report types to the FIU using the goAML portal. RHP must submit this report without delay, meaning as soon as reasonably possible after the transaction takes place or their suspicions develop. Please see also the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting* for further information.
Penalties	Violation of any statutory obligations may be subject to supervisory action, administrative and financial sanctions and penalties as deemed appropriate by the CBUAE.	

PART III: GUIDANCE FOR LFIs		
Understanding Risks	Circular 24/2019 requires that RHP must maintain an account with a bank operating in the UAE to be used for settlement and provide the CBUAE with its details. **The CBUAE expects LFIs to accept RHP customers**, but LFIs must manage the risk that these transactions create through the use of appropriate controls. LFIs must not accept as customers unregistered hawala providers based in the UAE, and must immediately report an STR to the FIU, inform CBUAE when they are detected, and closely monitor the relationship.	
Mitigating Risks	Risk-Based Approach	LFIs should take a risk-based approach to the preventive measures they put in place for all customers, including hawala providers. The approach should include at the minimum the conduct of an enterprise risk assessment, identification and assessment of the risks associated with specific customers, and the application of EDD and other preventive measures.
	CDD and EDD	Customer Identification and verification: LFIs are required to identify and verify the identity of all customers. Among other requirements, LFIs must physically check the original hawala provider registration certificate issued by the CBUAE and keep a copy thereof. LFIs should not form business relationships or conduct transactions with hawala providers without a valid registration certificate issued by the CBUAE (unregistered hawala providers).
		Beneficial Owner Identification: Where the hawala provider customers is a legal person, please consult the CBUAE's *Guidance for LFIs providing services to Legal Persons and Arrangements* for details on the identification of beneficial owners.
		Customer's Business and Business Relationship**:** It is critical that LFIs have processes and controls in place to ensure that they are able to identify hawaladar customers. LFIs must ensure that they fully understand their customers' source of funds and the business in which they are engaged, the intended use and expected activity on the account, to the extent that they can generally predict and identify activity that does not fit the profile.
		Ongoing Monitoring: All customers must be subject to ongoing monitoring throughout the business relationship to ensure that transactions are reasonable and legitimate. LFIs are required to ensure that the CDD information they hold on all customers is accurate, complete, and up-to-date. When customers are higher risk, including hawala provider customers, monitoring should be more frequent, intensive, and intrusive.
	Transaction Monitoring and Suspicious Transaction Reporting	Where possible, transaction monitoring systems used to monitor activity of the RHP should also be equipped to identify breaches of the permitted services by RHP. The transaction monitoring system used by LFIs should also be equipped to identify RHP that attempt to conceal activity from the LFI. LFIs must file a Suspicious Transaction Report, Suspicious Activity Report or other report types with the FIU when they have 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. Please see also the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting* for further information.
	Governance and Training	The specific preventive measures mentioned in this Guidance must take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces. As with all risks to which the LFI is exposed, a training program must ensure that employees are aware of the risks of hawala provider customers, familiar with the obligations of the LFI, and equipped to apply appropriate risk-based controls.