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

CBUAE OUTREACH EVENT
on the
AML/CFT Guidance for
LFIs Providing Services to
Registered Hawala Providers

24 August 2021

Outline of this Presentation

- Introduction
- Purpose and Structure of the Guidance Documents
- The Risk-Based Approach
- Customer Due Diligence
- Suspicious Transaction Reporting and Other Measures
- Q & A

Purpose & Applicability of the Guidance Document

Purpose

- This Guidance does NOT constitute new regulation and does NOT introduce new legal obligations.
- It is designed to help CBUAE's LFIs understand the purpose and context of their existing legal obligations, as well as the CBUAE's expectations for how those obligations will be fulfilled.
- The Guidance came into effect on 18 August, with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

Applicability

The guidance document applies **to Banks and Exchange Houses licensed by the CBUAE that provide services to Registered Hawala Providers.**

Regulation and Supervision of RHP in the UAE

The CBUAE permits legitimate Hawala Activity, being considered an important element in its continuous efforts to support financial inclusion and bring the unbanked population into the regulated financial system. Hawala is regulated by the Registered Hawala Providers Regulation issued by the CBUAE in 2019 ("Circular No. 24/2019"). RHP are supervised by the CBUAE, which 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, and to impose supervisory actions or administrative and financial sanctions for violations.

Regulation and Supervision of RHP in the UAE (cont'd)

Registration

- **All providers conducting hawala activity in the UAE must hold a Hawala Provider Certificate issued by the CBUAE.**
- It is not permitted to conduct hawala activity without being registered with the CBUAE.

Permitted and Non-Permitted Services by RHP

- RHP are **only permitted** to provide specified 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: (i) take deposits, exchange currencies, or sell or purchase travelers' cheques; (ii) provide any financial services other than money transfer services (e.g., loans, exchange of virtual assets); or (iii) execute transactions involving or on behalf of another RHP 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.

LFIs Providing Services to RHP

- **RHP must maintain an account with a bank operating in the UAE to be used for settlement** and provide the CBUAE with its details.
- <u>The CBUAE therefore expects LFIs to accept RHP customers, and LFIs should manage the risk that these transactions create through the use of appropriate controls.</u>
- **LFIs must not accept as customers unregistered hawala providers based in the UAE**, and must immediately report an STR to the FIU, inform the CBUAE when they are detected, and closely monitor the relationship.

Structure of the Guidance Document

The guidance document is divided into two main parts:

Understanding Risks

This section discusses why registered hawala providers (RHP) pose elevated risks to LFIs and describes aspects of these customers that increase or decrease their risk.

Mitigating Risks

This section discusses how LFIs can use *existing aspects* of their compliant AML/CFT programs to manage the specific risks of these customers.

Understanding Global Risks of Hawala Activity

Overview of Hawala Activity

- The FATF defines RHP—also known as *hawaladars*—as money transmitters that **arrange for the transfer and receipt of funds** or equivalent value and **settle through trade, cash, and long-term settlement**.
- Hawala is an activity based on trust and was established to **avoid high charges** by people who cannot afford them and to **reach beneficiaries in locations where banks do not operate**.
- Because communication is often by text message and there is no need for funds to clear, hawala transfers may also be available **faster** than transfers made using the formal financial system.
- 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 banks or exchange houses**, and possibly to use other financial services.

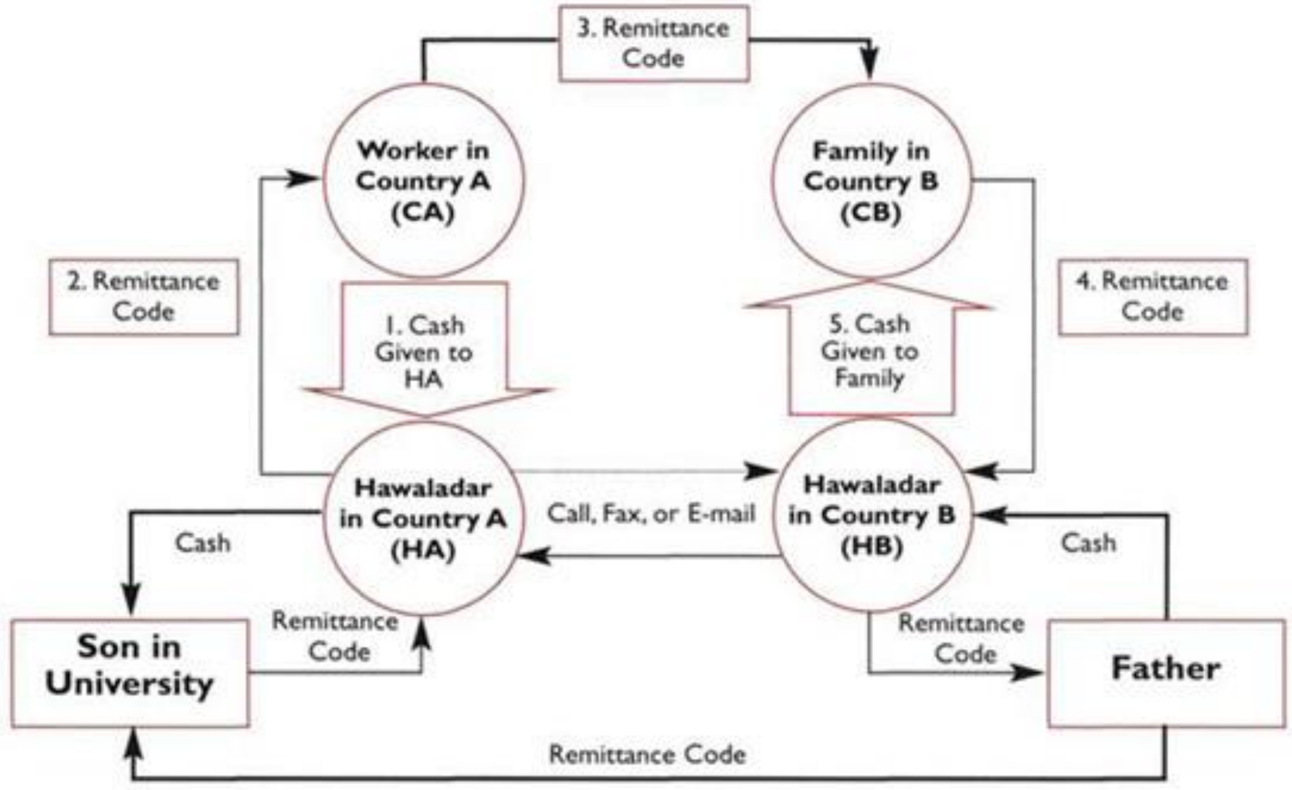
Other Common Attributes of RHP

RHP also commonly:

- **Operate in areas with high numbers of expatriates or migrant workers of a specific ethnic group**, where the RHP speaks the language and enjoys the trust of the community.
- **Operate with jurisdictions and regions underserved by other types of financial service providers**, such as high-risk areas experiencing war, civil unrest, conflict, economic crisis, or weak or non-existent banking systems.
- Operate as a hawala provider to facilitate remittance services **as a side business to other business activities**.
- Provide **one-off remittance services** and communicate with the customer only as much as needed to conduct the transaction.

Hawala Transactions

- In the top portion of the figure to the right, an expatriate worker (CA) uses a hawaladar (HA) to arrange a remittance to his or her home country.
  - The expatriate worker first makes a payment to HA in cash.
  - The hawaladar gives the worker a remittance code, which the worker then communicates to his or her family in country B.
  - HA then contacts a hawaladar counterpart (HB) in the receiving country, who arranges payment in local currency to the remitter's family or another beneficiary (CB).
- After the hawala remittance is completed, HA has a liability to HB, and HB has a claim on HA. The principals in the initial transaction do not play any role in the subsequent clearing and balancing of this position.
- HA and HB can settle their positions in various ways, including through "reverse" transactions, such as that depicted in the bottom portion of the figure, where HB facilitates the transfer of funds from a family member in country B to a family member in country A, or through bank transfers.



Source: IMF Report, "Informal Funds Transfer Systems"

Key Illicit Finance Risks of RHP

Regulatory & Controls Environment

- **Regulation of hawala providers varies greatly across jurisdictions**.
- Where hawala providers are not permitted, they may go **underground**—operating without AML/CFT controls and often presenting themselves as "general trading companies."
- Even where permitted and regulated, **RHP may not understand illicit finance risks or implement effective AML/CFT controls**.

Geography

- RHP are heavily exposed to the risks in the geographies where they **operate or have subsidiaries.**
- An RHP's geographic risk will also be impacted by the jurisdictions with which it most frequently **does business**, which may include jurisdictions with heightened illicit finance risks and weak or ineffective AML/CFT frameworks.

Products, Services, & Delivery Channels

- RHP provide money or value transfer services, which are inherently high risk.
- However, the risk of RHP transactions may still vary with the **size** and **purpose** of the transaction, or whether the RHP provides services through **anonymous** or **highly intermediated** channels, offers **other financial products**, or sells non-financial products for **cash**.

Customer Base

- RHP are likely to serve a customer base of lower-income individuals seeking to conduct or receive low-value transfers.
- However, such customers are not necessarily low risk, especially where they have **ties to jurisdictions that are high-risk for TF**.
- Risks are further heightened for customers that are **legal entities** or **politically exposed persons (PEPs)**.

Mitigating Risks

- ✓ Risk-Based Approach
- ✓ Customer Due Diligence and Enhanced Due Diligence
- ✓ Transaction Monitoring and STR Reporting
- ✓ Governance and Training

What is the Risk-Based Approach?

- LFIs are expected to **identify, assess, and understand** the money laundering, terrorist financing, proliferation financing, sanctions, and bribery and corruption risks (collectively, "illicit finance risks") to which they are exposed and **apply mitigating measures** that are commensurate with those risks.
- The risk-based approach (RBA) thus allows LFIs to adopt a **more flexible** set of measures in order to apply mitigating measures **more effectively**—directing greater human and technical resources to areas of heightened risk.
- LFIs should reflect the presence of higher-risk customers, including RHP, in their **enterprise risk assessments** and consider the strength of the controls in place to mitigate these risks.

Identifying and Assessing the Risks Associated with RHP

- LFIs should assess the risks of each customer to identify those that require enhanced due diligence (“EDD”) or more intensive or more frequent monitoring.
- In assessing the risks of an RHP customer, LFIs should consider:
  - **Controls risks**, including the regulatory requirements in place for the customer;
  - **Geographic risks** presented by the geographic location and footprint of the provider and its customers;
  - **Product, service, and delivery channel risks**, particularly where these promote the rapid, anonymous transfer of high values; and
  - **Customer risks**, including the proportion of high-risk customer types (e.g., PEPs, legal persons, and customers from high-risk jurisdictions) within the provider’s customer base.
- Questions an LFI may ask to determine the risk profile of an RHP customer include:
  - *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 AML/CFT 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?*

Customer Due Diligence

Customer Due Diligence: ID of Customers and Beneficial Owners

Customer Identification: LFIs are required to identify and verify the identity of all customers.

- When verifying an 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.
- 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.

Identification of Beneficial Owners: Where the hawala provider customer is a legal person, the LFI must identify and verify the identity of the RHP's beneficial owners, defined as any individual owning or controlling at least 25 percent of the legal person.

- Note that the threshold of beneficial ownership set forth in the AML-CFT Decision is a starting point for beneficial ownership identification.
- LFIs should assess whether identification of additional owners holding smaller stakes might assist them in managing the risk of a particular customer.

Customer Due Diligence: Purpose and Nature of the Account and Customer's Business

- The purpose of the account and the nature of the customer's business are critical drivers of risk for RHP customers. LFIs should fully understand how their customer makes money and what types of transactions it expect to carry out through the LFI's account.
- As they seek to understand the customer's business, LFIs should collect the information necessary to assess customer risk. This information is also critical to, and closely linked with, the customer risk rating process. LFIs should understand:
    - The jurisdiction(s) in which the customer is based or does business, including both the jurisdictional risk of crime and terrorism but also the regulations in place on hawala providers;
    - The products and services the customer supplies to its customers;
    - The customer's customer base;
    - The quality of the customer's AML/CFT controls, where they exist.

Key Risk Areas to Scrutinize at Onboarding

- Underground hawala providers often try to evade detection by creating new companies and/or frequently switching to new financial institutions. LFIs should therefore **screen the names of any new customer's beneficial owners, directors, and managers against internal watchlists of customers previously exited by the LFI.**
- LFIs should pay particular attention to the jurisdictions with which their hawala provider customer does business, and must **understand whether their customer offers financial services to other hawala providers** (e.g., whether it participates in clearing networks or makes transfers on behalf of the customers of another provider that lacks a network in certain jurisdictions).
- Furthermore, LFIs must fully **understand the intended use of expected activity on the account**, so that it can generally predict activity on the account and identify activity that does not fit the profile.
- LFIs must also **understand whether the hawala provider may be using the LFI's accounts to conduct business or move funds on behalf of customers** while attempting to conceal this activity from the LFI.

Customer Due Diligence: Ongoing Monitoring

Ongoing monitoring should be risk-based, so that higher-risk customers receive more frequent and intrusive monitoring.

- Ongoing monitoring should include both **a review and updating of customer information** held by the LFI, and **a review of the customer's account activity** since the last time the customer profile was updated, to ensure that the customer's transactions continue to fit the customer's profile and business.
- For higher-risk customers, LFIs should not rely solely on information supplied by the customer but should consider conducting searches of public databases and conducting interviews or site visits with the customer.

Ongoing monitoring also should be tailored to the <u>types</u> of risks identified during the customer risk-rating process and the risks inherent to the customer's structure, sector, or business.

- For RHP with complex ownership structures, LFIs should ensure that their understanding of the customer's ownership and control remains accurate and current.
- Similarly, LFIs should more carefully scrutinize the account activity of customers that are newly-formed entities or that are doing business in high-risk geographies.

Other Controls

Mitigating Risk: Suspicious Transaction Reporting and TFS

Suspicious Transaction Reporting

Where possible, LFIs should apply monitoring rules that are reasonably designed to alert on activity that may indicate that:

- A non-RHP customer is **acting as an unregistered hawaladar**; and
- An RHP is using the LFI's accounts **in breach of the services RHP are permitted to provide**, including by conducting business or moving funds on behalf of their customers or other hawala providers while attempting to conceal this activity from the LFI.

Red flags for concealed activity include the following:

- 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.

Implementation of TFS

- LFIs must screen all customers and their beneficial owners against sanctions lists, and should freeze any funds related to a designated person or a legal entity that is more than 50% owned or controlled by a designated person.

Mitigating Risk: Governance and Training

Training

- Training programs should educate employees about the risks faced by the LFI, including the particular risks associated with sectors and customer types to which the LFI has substantial exposure, including RHP where applicable.
- LFIs should develop dedicated training materials or programs for employees who frequently deal with such higher-risk customer types or sectors, whether within the compliance function or the business.

Governance

- Controls should be established within the context of a well-governed AML/CFT program, with clear roles and responsibilities, a qualified compliance officer, and substantive oversight by the Board and senior management.
- Where an LFI has developed a strong customer base in a certain sector, its AML/CFT compliance program should reflect this, and its compliance officer should be knowledgeable about those risks.

Questions