CBUAE OUTREACH EVENT
on the AML/CFT Guidance for Registered Hawala Providers

26 August 2021

Outline of this Presentation

- Introduction
- Purpose of the Guidance
- Hawala in the UAE
- Understanding Risk
- The Risk-Based AML/CFT Program
  - Risk Assessment
  - Governance and Training
  - Customer Due Diligence
  - Sanctions Implementation
  - Suspicious Transaction Reporting
  - Recordkeeping and Reporting
- Scenarios
- Q & A

About the Guidance

The Guidance came into effect on **18 August**, with Registered Hawala Providers expected to demonstrate compliance with its requirements within **one month** from this date.

The Guidance is designed to help Registered Hawala Providers understand:

- Their AML/CFT obligations;
- The risks they face in doing business; and
- CBUAE's expectations for how they will implement their AML/CFT programs.

Applicability

The guidance applies **to all Registered Hawala Providers**.

Hawala in the UAE

Regulation and Supervision of RHP by the CBUAE

- **The CBUAE permits legitimate Hawala Activity**, considering it an important element in its efforts to support financial inclusion and bring the unbanked population into the regulated financial system.
- **The CBUAE regulates Hawala Activity** with the Registered Hawala Providers Regulation issued by the CBUAE in 2019 ("Circular No. 24/2019").
- **The CBUAE supervises RHP** and has the right to examine the business of RHP and their agents and customers whenever it considers it appropriate to ensure proper compliance with their legal obligations.
- The CBUAE also has the power to take supervisory actions and to **impose administrative and financial sanctions for violations**.

Requirements for Hawala Providers

All hawala providers **MUST** hold a valid Hawala Provider Certificate issued by CBUAE!

Registration

Applicants must apply to the CBUAE for registration. They must be non-UAE nationals, officially residing in the UAE, and legally competent.

CBUAE Decision

CBUAE will notify the application whether the application was approved or rejected, with reasons for the decision.

Re-Registration

RHP must apply to renew their Certificate no less than **two months** before their current Certificate expires.

Operating Requirements

RHP must add Hawala Activity to their trade license, install required security systems, and register with FIU and CBUAE reporting systems. They must open an account with a UAE bank.

Permitted and Non-Permitted Services by Registered Hawala Providers in the UAE

- All RHP **MUST** maintain an account with a bank operating in the UAE to be used for settlement and provide the CBUAE with its details.
- RHP **CAN** conduct money transfers to support:
  - 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 **CANNOT**:
  - Take deposits, exchange currencies or sell and purchase travelers' cheques;
  - Provide 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 another 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.

Understanding Risks

Money Laundering

Under the UAE legal and regulatory framework, if you know that money or other funds are the proceeds of a crime, taking any of the following actions with respect to those funds is money laundering:

- Transferring or moving such proceeds or conducting any transaction with the aim of concealing or disguising their illegal source.
- Concealing or disguising the true nature, source or location of the proceeds as well as the method involving their disposition, movement, ownership of or rights with respect to said proceeds.
- Acquiring, possessing or using proceeds upon receipt.
- Assisting the perpetrator of the predicate offense to escape punishment.

Persons convicted of money laundering can be sentenced to up to ten years in prison and can be required to pay a fine between AED 100,000 and AED 5,000,000.

If the representatives or managers of a company commit money laundering on its behalf, the company can be fined up to AED 50,000,000.

Terrorist Financing

- Terrorist financing is providing an individual terrorist, or a terrorist group, with funds of any kind—not just money, but food, weapons, clothing—anything of value.
- Under the UAE legal and regulatory framework, all of the following constitutes terrorist financing:
  - Taking any of the actions in the definition of money laundering if you know that the funds are the property of a terrorist organization or terrorist, or are intended to finance a terrorist organization or terrorist.
  - Providing or collecting money when you know it will be used to commit a terrorist offense, or if you are doing so on behalf of a terrorist organization or terrorist.
- Terrorist financing is punishable by life imprisonment, or for a term no less than 10 years.

Sanctions Evasion

Targeted financial sanctions (TFS) are measures imposed by the United Nations Security Council (UNSC) or the UAE to prevent certain groups or individuals from having access to funds.

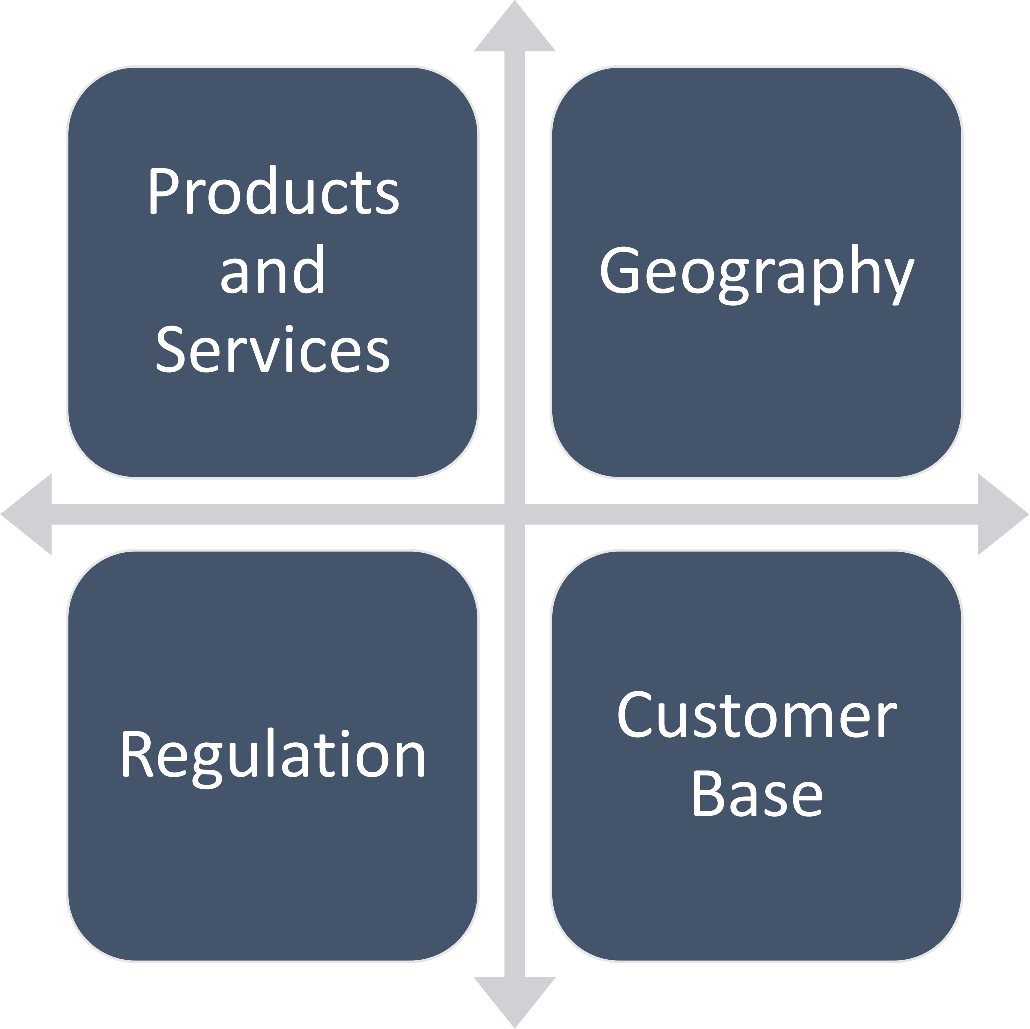
When a group or individual is subject to sanctions, it is a crime to provide that group or individual with any funds or financial services.

Violations of these prohibitions are punishable by imprisonment or a fine of up to AED 5,000,000.

ML and TF Risks to Hawala Providers

- Hawala providers, in the UAE and globally, have been abused by illicit actors seeking to launder the proceeds of crime, finance terrorism, and evade sanctions.
- All financial institutions are exposed to such risks. Like other financial institutions licensed by the CBUAE, RHPs are required by law to have certain programs in place to protect themselves from such abuse.

Sources of ML/TF Risk to Hawala Providers



Sources of ML/TF Risk to Hawala Providers, 2

Products and Services

- Hawala providers' essential service is quickly moving funds across borders.
- This service is a critical part of economic life and global commerce and takes place constantly all over the world.
- But it is also very attractive to illicit actors. Often, moving funds across borders quickly is their number one priority.

Geography

- Hawala providers provide an important service to UAE residents by serving parts of the world where big banks and exchange houses do not operate.
- Unfortunately, these parts of the world can present higher risks for money laundering and terrorist financing.

Sources of ML/TF Risk to Hawala Providers, 3

Regulation

- Registered Hawala Providers in the UAE are fully regulated and subject to the same AML/CFT requirements as other financial institutions.
- This is not the case throughout the world. Many hawala providers operate underground.
- Even if they are not illegal, they may only have a limited understanding of their obligations and use inadequate systems to comply with those obligations. This is not acceptable.

Customer Base

- Hawala providers serve customers who need to send money to their families or who are trying to run a business.
- But if your customers are engaging in money laundering and terrorist financing, you are exposed to their activities.
- If you are not diligent, you can end up helping them achieve their illegal goals.

The Risk-Based AML/CFT Program

Fundamentals of the Risk-Based Approach

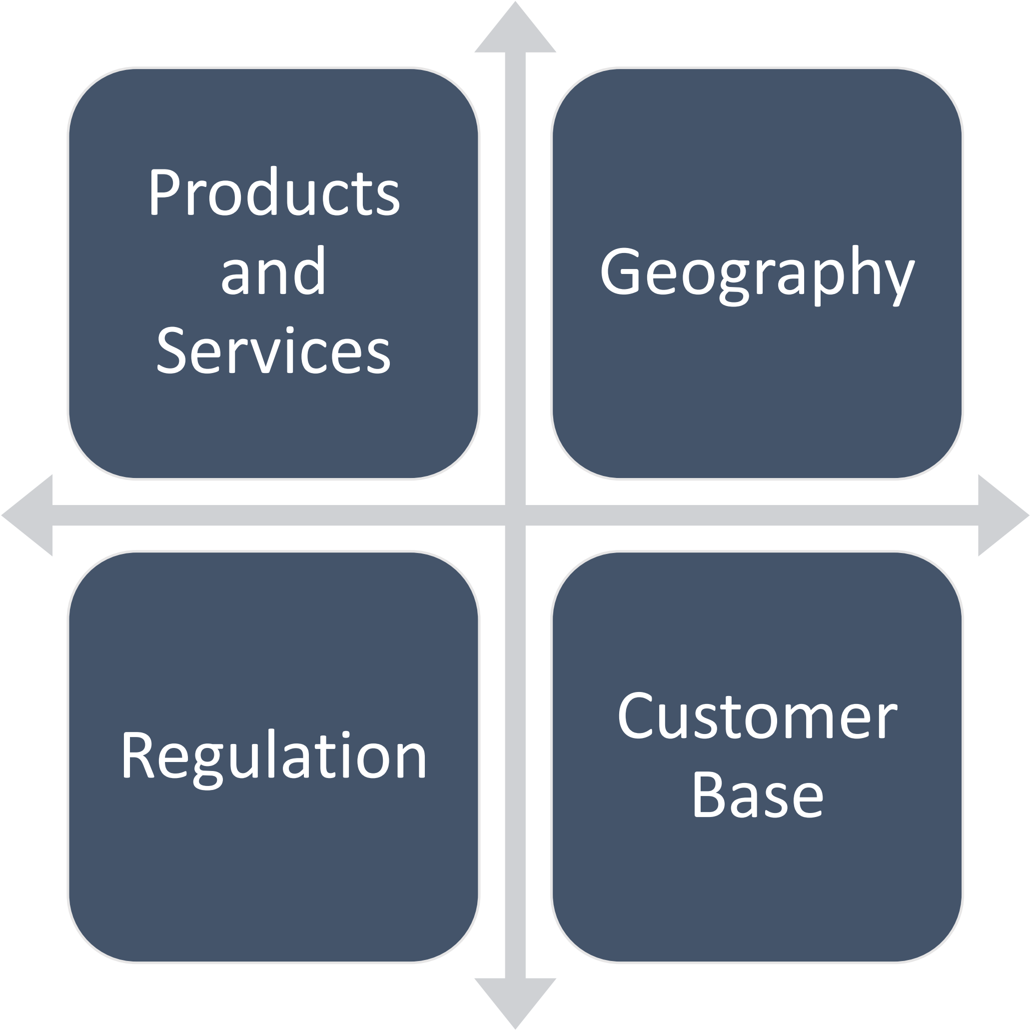
The Risk-Based Approach fundamentally means doing three things:

1. Understanding the risks to which you are specifically exposed as a business; and
2. Implementing an AML/CFT program that is designed to manage those risks, by
3. Devoting more resources to higher risks and putting in place controls that are specifically designed to target those risks.

Risk Assessment

The Risk Assessment (RA)

- The RA is the foundation of your AML/CFT program and a legal requirement. The RA is necessary to identify your risks and determine the nature and extent of the AML/CFT resources necessary to mitigate and manage those risks.
- The RA must consider:
  - Customer Risk
  - Geographic Risk
  - Products and Services Risk
  - Delivery Channel Risk
- The RA should take into consideration the **sector risks** we've discussed in this presentation, as well as the **specific risks** of your own unique business.
- There is no "one size fits all" RA, and you cannot use another institution's RA.



Governance and Training

Governance

- You must identify an employee of your business as the Compliance Officer in charge of your AML/CFT program.
- If your business has only one employee—you—then you are the Compliance Officer!
- The Compliance Officer must understand the legal requirements and the risks that your business faces.

Training

- The Compliance Officer must educate himself/herself on an ongoing basis in order to continually improve the program.
- The Officer must ensure that all employees understand their duties and responsibilities, and how they contribute to protecting the business.

Customer Due Diligence

Customer Identification

The purpose of customer due diligence (CDD) is to make sure that you have identified your customers so that you know with whom you are doing business. If you don't know this, you can't:

- Assess the risk;
- Implement sanctions;
- Assist law enforcement with any inquiries.

Customer identification is a legal requirement. **You must identify every single customer, no matter how long you have known them, how many times you've dealt with them, the nature of their transaction with you, or the quality of their references.**

A customer is anyone who uses the services you provide as a hawala provider.

Types of Customer Identification: Natural persons

CID

Collect full name, address, mobile #, nationality, DOB, ID type, and ID number.

CDD

All of the above, plus

Name of recipient/originator, and understanding of nature and purpose of the transaction.

EDD

All of the above, plus

Additional mandatory measures; and

Additional risk-based measures.

Types of Customer Identification: Legal Persons

When you conduct a transaction on behalf of a company, **the company is your customer**, not the person who comes into your shop.

CDD

- Name of the customer, legal form, address, trade license number, and senior managing official; plus
- Identification of the person representing the customer; plus
- Identifying beneficial owners and understanding control structure; and
- Understanding the customer’s business and the purpose of the transaction.

EDD

- **All of the above**, plus
- Additional mandatory steps.
- Additional risk-based steps.

Beneficial Owner Identification

- Companies can't think for themselves. All companies are controlled by human beings who make decisions and benefit from the company's activities.
- When you conduct a transaction on behalf of such a customer, you must identify and conduct CID on all **individuals** who own or control at least 25% of the customer.

Identifying Beneficial Owners

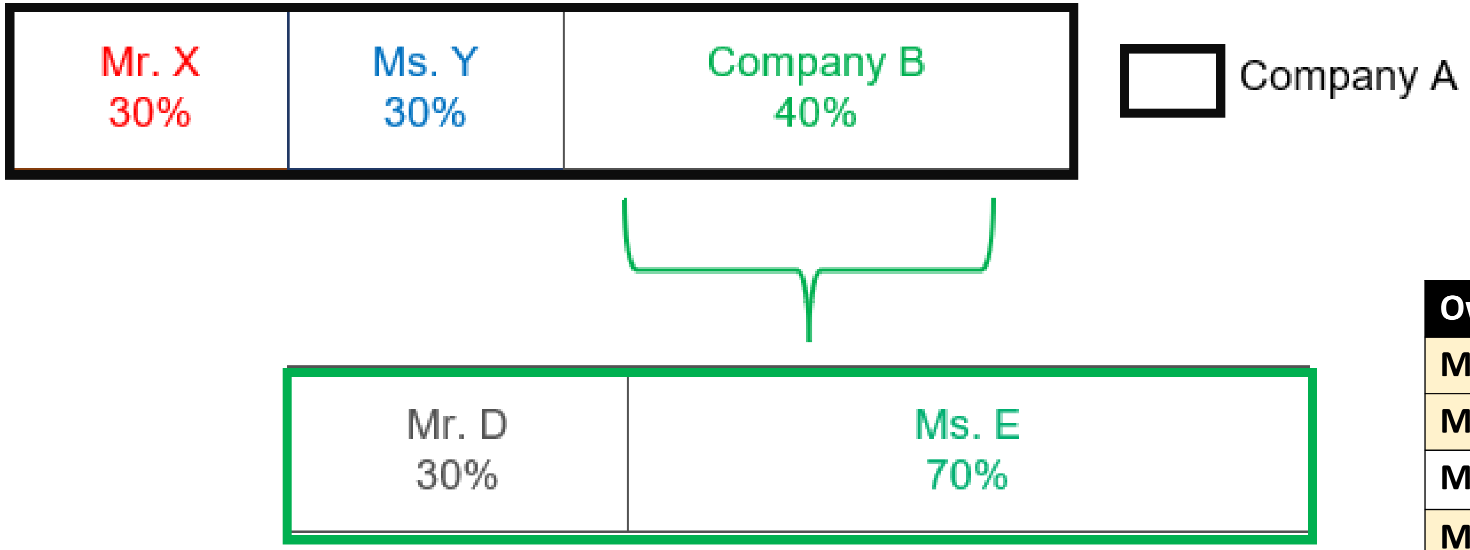
Simple Scenario

Mr. X 50%	Ms. Y 50%

Company A

Identifying Beneficial Owners

Indirect Ownership



Owner	Share	Source
Mr. X	30%	Ownership of Company A
Ms. Y	30%	Ownership of Company A
Mr. D	12%	Ownership of Company E
Ms. E	28%	Ownership of Company B

Must be ID'd as a beneficial owner

Purpose and Nature of the Transaction and Customer's Business

- RHP should obtain a clear understanding of the intended purpose and nature of the transaction in order to ensure that it does not breach the permitted services by RHP.
  - If they are not confident that the transaction is permitted, they should reject it.
- Because some businesses and sectors are higher risk for illicit finance than others, the nature of the customer's business is also a critical driver of risk.
- As they seek to understand the customer's business, RHP should collect the information necessary to assess customer risk. RHP should understand:
  - The jurisdiction(s) in which the customer is based or does business;
  - The sector in which the customer operates and the business it does;
  - The customer's customer base;
  - The quality of the customer's AML/CFT controls, where they exist.

Agent Due Diligence

- RHP are prohibited from using agents **in the UAE**.
- When you use **overseas** agents to conduct your business, including other hawala providers, you must treat them as your customers and perform Enhanced Due Diligence.
- Your agents can directly expose you to risk if they don't take proper precautions. As a result, there are specific requirements for EDD on agents.
- These requirements are designed to help you understand the risk to which you are exposed by your relationship with the agent, and whether the agent is acting appropriately to protect themselves and you.
- Specific requirements are described in the guidance.

Sanctions

Sanctions Implementation

By law, you are required to implement targeted financial sanctions within **24 hours** of the designation being announced—earlier if possible.

Implementation means:

- Not carrying out any transactions on behalf of a sanctioned person, or a legal person owned or controlled by a sanctioned person.
- Not transferring any funds to a sanctioned person.
- Not returning any funds in your possession to a sanctioned person, even if that person is the legal owner.
- Reporting any steps you have taken to implement sanctions, such as freezing funds or refusing to carry out a transaction, through goAML.

How do I Comply with Sanctions Requirements?

- You must screen all your customers against UNSC and UAE sanctions lists before:
  - Executing a transaction; or
  - Providing money to a customer that a third party has sent them.
- You must be certain to screen against the most up-to-date lists—the lists can change from day to day.
- You must screen not just the customer's name and address, but the names of its beneficial owners, the individual representing the customer (i.e., the individual in your shop), and the senior managing official you have identified as part of CDD.
- You may need to seek additional information from the customer in order to distinguish your customer from someone with the same name.

Transaction Monitoring and Reporting

FIU Reporting

- Reporting suspicious transactions or activities to the FIU is a critical part of the AML/CFT program.
- RHP must report without delay any behavior that they reasonably suspect may be linked to money laundering, the financing of terrorism, or a criminal offence to the FIU through goAML.
- These reports help the FIU and potentially police and prosecutors investigate criminal behavior and protect the UAE.
- Filing a report does not mean that your program has failed—it means your AML/CFT program has succeeded, because you have identified suspicious behavior.
- You must never tell anyone except the authorities that you have filed a report.

Identifying Suspicious Transactions and Activities

What is a Suspicious Transaction or Activity?

- You do not need to know for certain that behavior is linked to a crime before you report. In fact, you should not wait until you know this.
- You should report any behavior that does not have a legitimate explanation.
- You should take reasonable steps to investigate the behavior, but you are not required to be a detective.

How do I Identify One?

- Your system for identifying these transactions depends on the size and complexity of your business, but should be capable of consistently identifying unusual activity.
- The largest RHPs should have an automated system that surveys all transactions and alerts on those that may be indicators of illicit activity.
- Smaller RHPs can consider each transaction individually.

Identifying Suspicious Transactions and Activities, 2

The following are situations in which you should strongly consider filing an STR/SAR with the FIU. This list is not complete—you must always use your judgment and be watchful for behavior that has no clear legitimate explanation.

- 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.
- 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 attempting to order transactions that RHP are not permitted to carry out.

Recordkeeping and Reporting

Recordkeeping

You must maintain the following records for at least five years:

- You must maintain specific information for when sending or receiving a remittance.
- Your partners must also provide this same information before you can complete a transfer they originate.
- Transaction records, CDD records, and copies of STRs/SARs.

Reporting

In addition to STRs, you must make the following reports:

- Daily Reporting via the RRS.
- Quarterly Reporting of settlement accounts to CBUAE.

Putting it Together: Scenarios

Individual enters the shop

- Understand the services the individual wants.
- Make sure these services are permitted.
- Understand individual’s relationship to the customer.

CDD

- Collect required customer information.
- Consider whether everything you know about the transaction makes sense when taken together.

Conduct Transaction

Transmit required originator and beneficiary information with transaction.

Recordkeeping

- Maintain records of CDD, information accompanying the transaction, and transaction information.
- Report transaction through RRS.

Individual enters the shop

- Understand the services the individual wants.
- Make sure these services are permitted.
- Understand individual’s relationship to the customer.

CDD

- Collect required customer information.
- Customer’s stated income is not consistent with transaction value.
- Customer cannot provide a satisfactory explanation.

File SAR

- Report through goAML.
- Provide all information you can about the customer and attempted transaction.
- Place customer on watchlist.

Types of reports to be submitted to FIU:

1- Suspicious Transaction Report (STR):
This report is raised when the reporting entity is suspecting a transaction. Minimum Requirements: Remitter & Beneficiary Name, Identifications Numbers, Identifications copies**(EID and/or Passport)**, details of the suspicion, and actions taken by RE).

2- Suspicious Activity Report (SAR):
This report is raised when the reporting entity is suspecting an activity. Minimum Requirements: Customer's name, Identifications Numbers, Identifications copies**(EID and/or Passport)**, details of the suspicion, and actions taken by RE).

3- Fund Freeze Report (FFR):
This report is raised when the reporting entity finds a full match of customer's name with a name listed in: **UAE SANCTIONS LIST & UN SANCTIONS LIST.**

4- Partial Name Match Report (PNMR):
This report is raised when the reporting entity cannot verify if the name of the customer is a full match to the name of a sanctioned person listed in: **UAE SANCTIONS LIST & UN SANCTIONS LIST**.

Related Links:

For Technical issues related to goAML, contact:
goAML@uaefiu.gov.ae

For UAE SANCTIONS LIST & UN SANCTIONS LIST:

www.uaeiec.gov.ae