



Strategic Analysis Report
Abuse of Legal Entities
In Money Laundering and Terrorist Financing
UAE-FIU
2021

Financial Intelligence Unit, P. O. Box 854, King Abdullah Bin Abdulaziz Al Saud ST, Abu Dhabi, UAE.

Phone no: +97126919955

Email address: uaefiu@uaefiu.gov.ae

TABLE OF CONTENTS:

Content and objectives	3
Methodology	4
List of Acronyms	5
Terms & Definitions	5
EXECUTIVE SUMMARY	6
INTRODUCTION.....	7
1. OVERVIEW OF THE RELEVANT DATA AND INFORMATION UNDERLYING THE STRATEGIC ANALYSIS.....	9
2. MAIN TRENDS AND TYPOLOGIES.....	11
3. LINKS BETWEEN THE ABUSE OF LEGAL ENTITIES AND OTHER RISK-FACTORS.....	13
4. INDICATORS AND GUIDANCE FOR THE REPORTING ENTITIES.....	13
5. EXAMPLE CASES.....	15
CONCLUSION.....	19

CONTENT AND OBJECTIVES

This Project is part of the Strategic Analysis Plan (SAP) adopted by the UAE FIU considering the requirements of the *National Assessment of Inherent Money Laundering and Terrorist Financing Risks in the United Arab Emirates* (NRA) and following *UAE National Action Plan (NAP) to Implement the Anti-Money Laundering and Combatting Terrorism Financing National Strategy 2020-2023*.

This Report presents the results of the strategic analysis related to the Legal entities (LEs) registered and/or operating in the UAE and their possible abuse in the context of Money Laundering (ML) and Terrorist Financing (TF) schemes, including the exploitation of Trade-based Money Laundering (TBML) and disguising of illicit funds or “dirty money”.

The purpose of this Report is to:

- Identify Trends and Typologies of abuse of LEs for ML/TF purposes; and
- Develop Indicators and Guidance for the Reporting Entities (REs).

UAE FIU intends to promote the highest level of awareness and knowledge of the phenomenon by the public and private sectors. And to create the best conditions for the enhancement of the cooperation and information sharing with the counterpart Financial Intelligence Units (FIUs) to manage and mitigate the relevant risks at the cross-border and international levels.

METHODOLOGY

Analysis has been carried out based on the Strategic Analysis Methodology adopted by the UAE FIU, ensuring a structured and comprehensive risk-based approach, in view of developing raw data and information into knowledge and intelligence to be used in policy and decision-making processes, as well as operational activities.

The analysis and conclusions illustrated in this Report are based on the analysis of data and information held by the UAE FIU, other data and information obtained from other domestic and international sources, particularly in the period 2020-2021 (May).¹

¹ The data and information analyzed include but are not limited to: STRs and SARs databases; Cash declarations; information received from UAE Authorities; information received from counterpart FIUs.

LIST OF ACRONYMS

TERMS DEFINITIONS	& Description
ML/TF	Money Laundering and Terrorist Financing
UAE-FIU	Financial Intelligence Unit of the UAE
LE	Legal Entity
FI	Financial Institution
DNFBPs	Designated Non-Financial Businesses and Professions
LEA	Law Enforcement Authority
ECDD	Enhanced Customer Due Diligence
CDD	Customer Due Diligence
KYC	Know Your Customer
goAML	The Financial Intelligence Unit online reporting application
STR	Suspicious Transaction Report
SAR	Suspicious Activity Report
SD	Spontaneous Dissemination
RFI	Request for Information
RE	Reporting Entity
PEP	Politically Exposed Person
PP	Public Prosecution
JP	Juridical Person
NP	Natural Person

EXECUTIVE SUMMARY

UAE is a country with diverse and multicultural population with a secure and stable economy and strong institutions. As such, the UAE has an accessible financial system, a strategic geographic location between Asia, Europe, the Middle East, and Africa and is a well-developed international trading and financial hub.

There are over 500,000 Legal Entities (LEs) established in the UAE. While LEs are generally established for licit purposes, the analysis suggests that they are still vulnerable and can be abused for illicit purposes, considering some gaps in the identification of the Ultimate Beneficial Ownership (UBO), the extensive use of cash and the recurrence of complex international schemes.

In this context, the risk raised from LEs potential vulnerabilities can be viewed based on multiple components, in particular the following two: the type of LE, and the LE's jurisdiction (Mainland or Free Zone).

The relevant data and information show also some shortcomings related to the quality of the Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) and capability of the Reporting Entities (REs) to detect and effectively report the relevant suspicious transactions and activities.

The UAEFIU has developed specific indicators and Guidance for the Reporting Entities in view of effectively detecting and reporting cases of possible abuse of LEs for ML/TF and other illicit purposes.

Selected example cases show how LEs have been abused in concrete ML/TF scenarios and how the UAEFIU and other UAE authorities countered these threats.

INTRODUCTION

In the context of the UAE, the notion of LE refers to any form of company, corporation, organization, or business enterprise that provides services, goods, products, or that is used for any other purposes.

The number of LEs registered in the UAE was 401,013 in 2017. While in 2021, the number of LEs has risen to 569,393, with an increase of 93% both in the Mainland and in the Free Zones, and a presumable increase of the related risks in the background.

LEs are relatively easy to establish in the UAE. Whilst LEs are generally established for licit purposes, they are still vulnerable and can be abused for illicit purposes. Money launderers tend to use LEs to launder the proceeds of a crime – or a series of crimes – due to different vulnerabilities, often exacerbated by the inadequate fulfilment of Customer Due Diligence (CDD) and Know Your Customers (KYC) requirements, making the identification of the Ultimate Beneficial Ownership (UBO) more difficult, particularly in cases of complex international structures.

One further factor cannot be underestimated in this context, namely the extensive business activities and opportunities that exist in the UAE economy. This is a prospective for licit activities but also a golden chance for ML and TBML, and for Terrorist Organizations to exploit a wide range of economic and financial opportunities in the Country for illicit purposes.

This Report is structured as follows:

- **Section 1 – Overview of the relevant Data and Information underlying the Strategic Analysis.** This Section provides an overview of the main sources underlying the strategic analysis related to Legal Entities (LEs) and the link between the abuse of LEs and ML/TF schemes, including some of the key features, such as the types of transactions and activities carried out by LEs, the volume of transactions, and the main Jurisdictions involved.

This Section also emphasizes on the possible shortcomings related to the quality of the STRs and SARs in connection with the current list of indicators or '*Reason For Reporting*'.

It finally considers possible links between the abuse of LEs and other relevant elements and risk factors, such as:

- › Identification of Ultimate Beneficial Owner (UBO);
 - › Trade Based Money Laundering (TBML);
 - › Complex ownership structure;
 - › Political Exposed Persons (PEPs).
- **Section 2 – Main Trends and Typologies.** This Section illustrates the main types, methods and techniques implemented to abuse LEs for illicit purposes, and the main trends and typologies detected.
- **Section 3 – Links between the abuse of Legal Entities and other risk factors.** This Section describes the links between the abuse of LEs and other risk factors, particularly the use of cash. Based on information sharing with UAE Authorities, LEs and the correlation with elicited crimes, number of requests received on LEs vis-à-vis 'Natural Persons' (NPs), and summary of 'Cash Declarations' related to LEs.
- **Section 4 – Indicators and Guidance for the Reporting Entities.** This Section includes developed Indicators and Guidance for the Reporting Entities in view of effectively detecting and reporting cases of possible abuse of LEs for ML/TF and other illicit purposes.
- **Section 5 – Example Cases.** This Section presents sanitized cases showing how LEs have been abused in concrete scenarios and how the UAE FIU and other UAE Authorities countered the threats.
- **Conclusion.**

1. OVERVIEW OF THE RELEVANT DATA AND INFORMATION UNDERLYING THE STRATEGIC ANALYSIS

The analysis presented in this Report are based on a broad range of data and information, including, but not limited to, the databases owned or directly accessible by the UAE FIU particularly the Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) database. The data and information requests received from UAE Authorities – such as the Federal Public Prosecution, Local Police Departments, the Federal Customs Authority (FCA) and counterpart Financial Intelligence Units (FIUs), particularly in the period 2020–2021 (May).

Additional information has been requested from selected Reporting Entities (REs), which provided the UAE FIU with useful inputs contributing to the ongoing analysis.

The UAE FIU analyzed all the available and obtainable data and information to assess possible links between LEs and ML/TF and to identify the main trends and typologies (see Section 2).

1.1. Main risk-factors

The review of STRs and SARs shows some recurrent patterns and links between the abuse of LEs and other elements and risk factors, such as:

(a) Identification of Ultimate Beneficial Owner (UBO)

Most of the STRs relating to LEs lack UBO details. Possible reasons could be the intention of the customer (or counterpart) to hide this information, or the lack of adequate knowledge by the RE of the definition of UBO and deficiencies in the fulfilment of the requirements relating to the identification of the UBO.

(b) Trade Based Money Laundering (TBML)

Different elements indicate a direct connection between the abuse of LEs and TBML. Generally, the significant value of unjustifiable remittances and rapid movement of funds in the accounts have initially triggered REs’

investigation/review of the account. Other triggers are recurrent such as; negative news/derogatory remarks on owner(s), director(s) or shareholder(s), providing forged invoices, discrepancies in shipping documents, etc.

(c) Complex ownership structure

Many STRs relating to LEs reported ownership structures are unnecessarily complex and illogic, in addition of involvement of offshore companies. Some key features noted to be used is having several layers in the ownership chain and appointing overseas Entities as shareholders, for example; ABC Entity (established in Mainland) owned by EFG Entity (registered in Free Zone), which is ultimately owned by an overseas Entity of which the UBO is unknown.

(d) Politically Exposed Persons (PEPs)

Data and information analyzed do not show a strong link between PEPs and abuse of LEs. However, this possible link, given its implications, is the object of regular monitoring and analysis at the operational and strategic levels.

1.2. Other vulnerabilities relating to CDD and KYC requirements

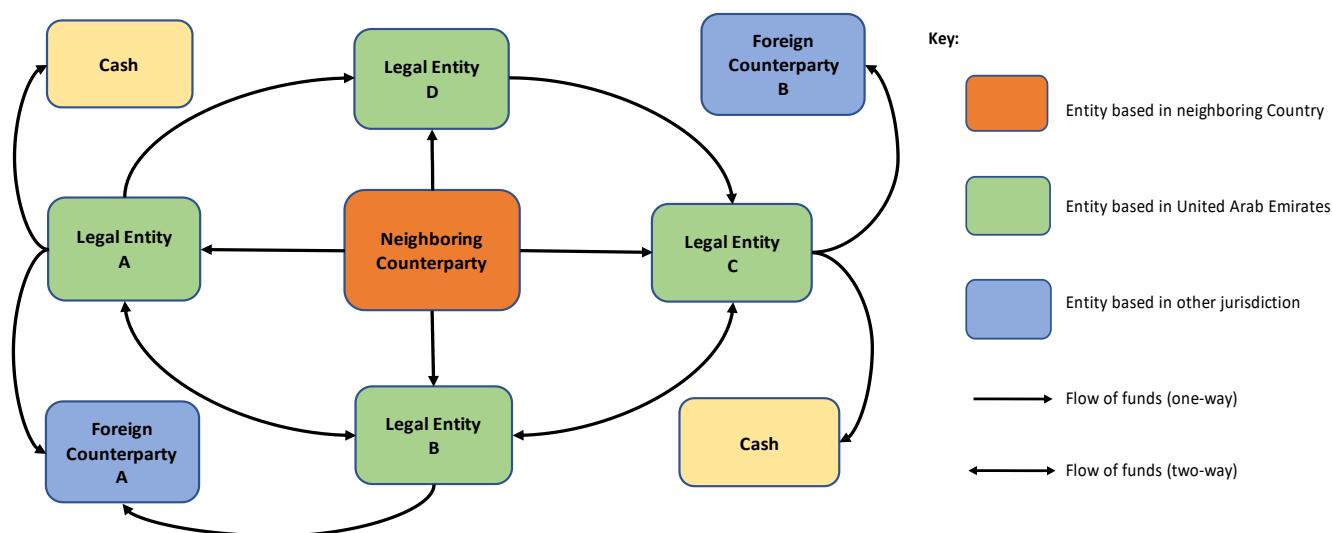
A vital element of this review was the information obtained from Reporting Entities as well as the content of received suspicious reports. In light of that, some concerns on the overall quality of reports were observed, pertaining to Deficiencies in the fulfilment of Customer Due Diligence (CDD) and Know Your Customers (KYC) requirements. The deficiencies in the fulfilment of the CDD and KYC requirements may create a cascading effect on identification of domestic and foreign PEPs (including their close associates and relatives as defined by the UAE legislation) owning LEs abused for illicit purposes.

2. MAIN TRENDS AND TYPOLOGIES

The analysis shows one main typology of abuse of LEs for illicit purposes.

LEs domiciled in UAE receive remittances from counterparties located in a neighboring country (most of them LEs). The funds subsequently rotated through multiple entities' accounts within the UAE, and either remitted to entities located in different jurisdictions (including high-risk jurisdictions), or interrupted via Cash withdrawals.

Simplified Illustration of Typology:



In-depth analysis of a sample of approximately 400 STRs allowed the identification of the following recurrent elements:

- Repeated 'purpose' of remittance used for the wire transfers received from neighboring Country stated as "purchase of goods".
- Commonly observed irregularities on the supporting documents presented to the REs by the customer, i.e. duplicate invoices, discrepancies in

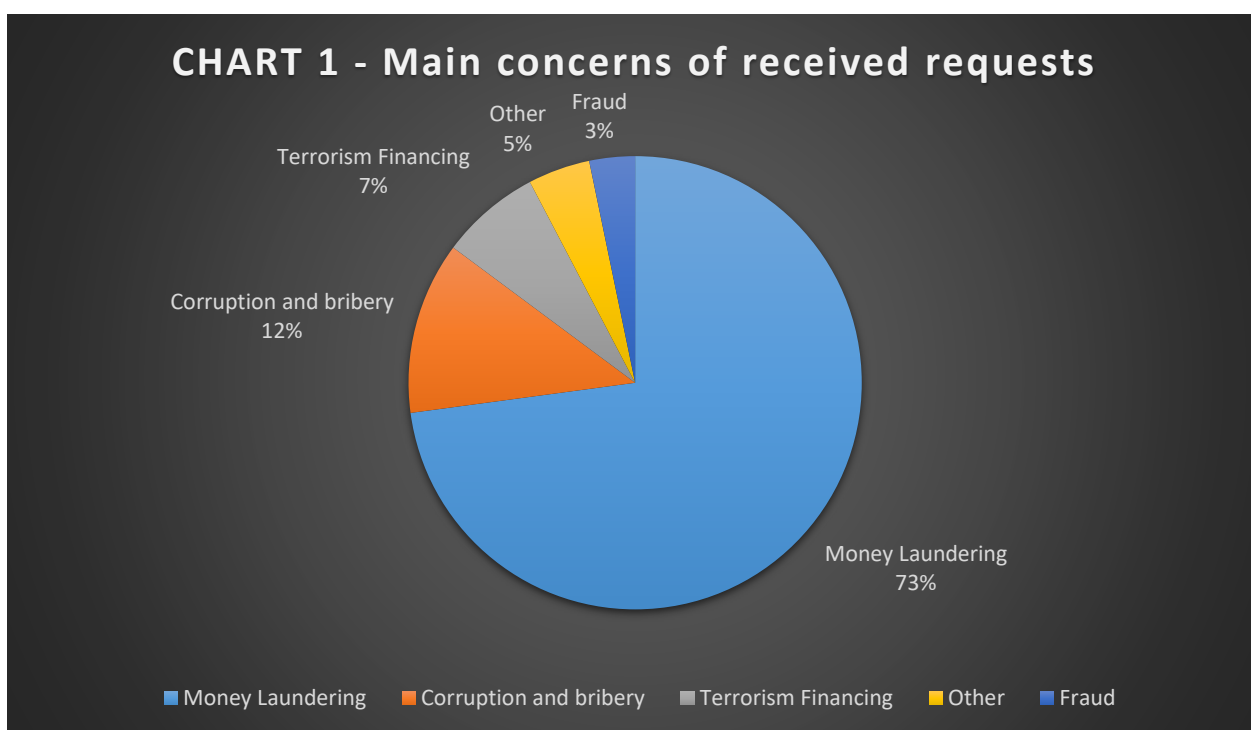
transaction dates and invoice sequence, item descriptions are too generic, no indicated payment mode, etc.

- Absence of transportation documents to ascertain movement of goods. Shipments are claimed to be handled by buyers (counterparties located in the neighboring country) through an intermediary and are transported via land.
- The date of incorporation of UAE domiciled LEs was mainly in 2019, and were predominantly into “electronics trading” and “building materials trading”.
- Majority of involved Entities were formed as ‘Limited Liability Company’.
- Local bank accounts involved were mostly newly opened, and appear to be funnel accounts (Pass-through nature).
- Funds withdrawn as cash are justified as “payment to suppliers” based on supplier request for payments to be in Cash as opposed to other instruments.
- Funds transferred internationally were directed to more than 200 foreign counterparties in various jurisdictions, that are engaged in different lines of business and have no apparent relationship with the senders.
- Possible links identified connecting reported counterparties with designated sanctioned countries.

3. LINKS BETWEEN THE ABUSE OF LEGAL ENTITIES AND OTHER RISK-FACTORS

The exchange of information with other UAE Authorities shows links between the abuse of LEs and other risk factors, particularly the use of cash as already noted.

The UAE FIU received a total number of 4,985 inquiries during the period from January 1, 2020 until May 31, 2021. 20% of the said requests relate to LEs, and were concerning multiple crimes as illustrated in the chart below (Chart 1).



(Chart 1)



4. INDICATORS AND GUIDANCE FOR THE REPORTING ENTITIES

The establishment of risk indicators related to LEs aims to guide the reporting entities with activity or transactions indicative of a potential illicit activity. The presence of an indicator in a situation can raise suspicions and trigger investigation leading to further identification of other indicators.

However, a criminal activity cannot be explicitly inferred based on a single indicator, but a simultaneous occurrence of it along with analysis of other available information may suggest that a LE is being potentially abused for ML/TF purposes.

Here are some indicators that could possibly alert the risk of misusing Legal Entities for ML/TF:

- Transactions that appear more complicated by use of impressive but nonsensical terms.
- Circulation of funds between linked or related entities accounts using different type of instruments (cheques, electronic transfers, etc.).
- Large volume of cash transactions through different branches of the financial institution, specially conducted by multiple individuals.
- Transactions structure appears unnecessarily layered and designed to obscure the true origin of funds.
- Multiple parties collaborating in a single transaction.
- Multiple entities remitting a single or repeated beneficiary (also entity) of which the funds subsequently remitted to offshore entity.

- A legal entity is reluctant to provide substantial information about the business nature and purpose, anticipated account activity and other relevant information at the account opening date and/or throughout the business relationship.
- A legal entity does not have adequate presence or the mere presence conveys ambiguity, i.e. online presence through websites that are vague.
- A legal entity has a UBO or associates with known dealings with counterparties residing in high risk or sanctioned jurisdictions.
- A legal entity or its UBO is linked to negative/adverse media reports.
- A legal entity has a peculiar structure that is unreasonable and complex, i.e. potential involvement in shell companies, a parent or subsidiary of an offshore company.
- A legal entity uses intermediary or third-party extensively with no reasonable justification and providing inadequate supporting documents when requested to sustain the source and prove legitimacy of the transactions.
- A legal entity is newly established and observed to have engaged imminently to high volume of transactions and business activities.

5. EXAMPLE CASES

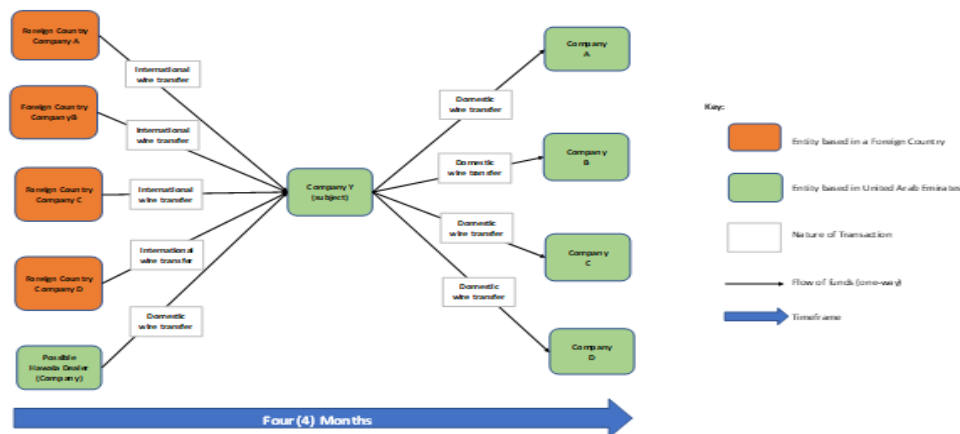
The following example cases show how LEs have been abused in concrete ML and TF scenarios and how the UAE FIU and other UAE Authorities countered the threats.

Case 1 - Possible Money Laundering through LEs

UAEFIU has received an STR from a local bank in the UAE against Company Y, mainly due to rapid movement of funds observed in its account. Company Y is a Goods Wholesale Retailer, whose UBO is from a high-risk jurisdiction. Company Y has received high value of funds from 56 companies residing in Foreign Country A, which reached up to AED 1 Billion in a span of four months. In addition, funds received from other local companies identified as 'hawaladars'.

Funds mainly dissipated as transfers to more than 35 local counterparties, on which the RE had concerns related to ML and possible sanctions evasion. Company Y did not provide supporting documents to ascertain the purpose of payments and business relationships with local companies. The reporting entity decided to mitigate the risk associated with their customer and exited the relationship with Company Y.

Simplified Illustration:



The UAE FIU disseminated a report to the relevant Police Department for further investigation on the involved subjects. The Police responded that the case is classified with high importance and the indicators denote occurrence of a suspicious activity, and requested UAE FIU to reach out to Foreign Country A's FIU for additional information. Further, the Police is in the process of investigating the subjects involved and coordinating with Foreign Country A through the appropriate channels, to identify any link of the funds transferred to UAE entities to a possible criminal activity in Foreign Country A.

Risk Indicators:

- Declared annual turnover was huge which is very unusual for a newly established company (Company Y).
- Sudden surge observed in the account activity – 1,496 transfers received from 56 entities based in foreign jurisdiction (Country A) in a short period of time.
- Transactions seemingly of pass-through nature – funds received directly debited via wire transfers leaving low balance in the account.
- Links to other STRs with same suspicions and/or reasons for reporting.

- Counterparties details were not disclosed during onboarding of customer (gaps in CDD).
- No transportation documents provided to ascertain movement of goods related to payments.
- Unable to identify counterparties' nature of business.
- Similar concerns received from counterpart FIU in Country A, on entities remitting funds to other entities located in the UAE.

Case 2 - Possible Terrorist Financing through LEs

The UAE FIU received multiple STRs/SARs on a General Trading Entity named; (Company E), its owner (who is xx National) and a subsidiary company named; (Company P) which is involved in multiple business activities. The main selected "reason for reporting" of the received STRs/SARs were related to adverse media reports, sudden increase of unjustified transactions activities in the account, and involvement of Third-party payments. During the analysis carried by UAE FIU, links established between the reported subjects and an Entity (Company MH) listed as 'Specially Designated Global Terrorist' and believed to be linked with a known terrorist group. Since Company MH does not have a presence in the UAE, and in addition to other facts, it was suspected that Company E and Company P along with other associated entities based in the UAE are conducting trade and financial transactions on behalf of Company MH. The UAE FIU initiated a Freeze instruction (with the approval of H.E. The Governor) on related accounts based on possible Terrorist Financing and sent a request to Public Prosecution to continue the Freeze order. Case disseminated to State Security Prosecution for further investigation and conviction.

Risk Indicators:

- The reported subjects were linked to other Entities on which STRs/SARs have been raised.
- Sudden surge observed in the account activity.
- Large amount of cash transactions involved (deposits and withdrawals) of which the source and destination was unknown.
- Payments observed in the accounts were sent against "Insurance Policy". While other payments received were from "Life Insurance" companies.
- Large cash amounts were transferred through Exchange House to different parties in other jurisdictions.
- The reported subjects found to have numerous accounts/relationships with multiple Banks and Exchange Houses without any rationale.
- Many of the related entities are sharing the same addresses.

CONCLUSION

In conclusion, criminals and money launderers constantly explore and exploit different methods in their benefit. Though it is noted that LEs are being targeted and abused in illicit acts, genuine LEs may also stand as conduit for ML/TF.

Willingly or unwillingly, LEs are used in co-mingling illegitimate funds with legitimate business funds, changing the form of such funds, or even moving the funds from one jurisdiction to another; all in attempt to deprive such assets/funds from the origin source and the true ownership and harden the ability to trace such assets by LEAs. The easy passage of funds and the variety of financial and trade transactions available found to be an ideal vehicle for the 'layering' stage of Money Laundering.

On the other hand, criminals hiding behind a 'front company' or a 'shell company', which are companies that appear as legitimate but actually controlled by criminals, expose various sectors other than the financial system. Accessing sectors like Real Estate, Securities and Commodities, etc. provides a high opportunity for criminals to re-enter the illicit funds into the economy, via what is known as the 'integration' stage of Money Laundering.

Intentionally using complex ownership structure, collaborating domestic with foreign entities, easily changing shareholders or business names are other factors entailed in increasing the risk of concealing the information of real ownership (UBO).

The UAE FIU emphasizes on the importance of the aforementioned risk factors and developed indicators mentioned in this report, for REs and relevant UAE Authorities to consider while developing or updating current ML/TF combating programs.