وحدة المعلومات المالية
Financial Intelligence Unit

The Abuse of Legal Persons and Arrangements in Illicit Activities

A Strategic Analysis Report

Second Edition - March 2023

UAE Financial Intelligence Unit – P.O.Box 854, Al Karamah Street – International Tower, Abu Dhabi.

Phone No: +97126919955

Email address: uaefiu@uaefiu.gov.ae

Disclaimer

For any enquiries regarding this document, please contact rsas@uaefiu.gov.ae.

TABLE OF CONTENTS

LIST OF ACRONYMS

CBUAE	Central Bank of the UAE
CSP	Company Service Provider
DNFBPs	Designated Non-Financial Businesses or Professions
DPMS	Dealers in Precious Metals and Stones
ICP	Federal Authority for Identity, Citizenship, Customs and Port Security
FIs	Financial Institutions
FPP	Federal Public Prosecution
GoAML	The Financial Intelligence Unit Reporting System
HRCA	High-Risk Country Activity
IACAD	Islamic Affairs and Charitable Activities Department
IEMS	Integrated Enquiry Management System
LEA	Law Enforcement Authority
LE	Legal Entity
LP	Legal Person
ML	Money Laundering
MOCD	Ministry of Community Development
MOE	Ministry of Economy
MOI	Ministry of Interior
NPOs	Non-Profit Organizations
PEP	Politically Exposed Person
PF	Proliferation Financing
PMS	Precious Metals and Stones
PP	Public Prosecution
RE	Reporting Entity
RFI	Request for Information
RFR	Reason for Reporting
RHP	Registered Hawala Provider
RSAS	Research and Strategic Analysis Section
SAR	Suspicious Activity Report
SD	Spontaneous Dissemination
STR	Suspicious Transaction Report
TF	Terrorist Financing
UBO	Ultimate Beneficial Owner
UAEFIU	The UAE Financial Intelligence Unit
UHP	Unregistered Hawala Provider

EXECUTIVE SUMMARY

Over the past two years, the UAEFIU has issued a number of strategic analysis reports on the abuse of legal persons in money laundering, trade-based money laundering (TBML), professional money laundering (PML), and foreign proceeds of crime, as well as the abuse of dealers in precious metals and stones in illegal activities, among others. This report extended the previous strategic analysis work to identify further typologies and patterns related to the possible abuse of legal persons and arrangements in illegal activities. The findings of this report were based on 14 hypotheses drawn from the UAE National Risk Assessment (NRA), the Legal Persons and Arrangements Risk Assessment, and patterns observed globally and published in other jurisdictions' case studies.

From 1 January 2021 to 31 December 2022, the UAEFIU received **13910** out of 48416 Suspicious Transaction Reports (STRs) involving legal entities in suspicious transactions. Out of said 13910 STRs, **6,461** were directly related to when a legal entity was involved as either a subject or a counterpart (be it as a sender or recipient or both). In addition, **1,694** out of 8503 Suspicious Activity Reports (SARs) were received during the same period in which a legal entity was involved as either a subject or a counterpart or both. Out of said suspicious reports, **202** cases were disseminated to Law Enforcement Authorities (LEAs), noting that a case may combine one or more suspicious reports. The cases related to legal persons constituted approximately **57%** of the total disseminated cases.

A sample of **819** STRs/SARs were examined, representing 10% of the total reported STRs/SARs associated with legal persons during the examined period. These are in addition to **80** reports related to high-risk country activities (HRCA) that were received from registrars, as well as **157** reports related to international cooperation (Inward SDs, Inward RFIs, Outward SDs, and Outward RFIs), representing 10% of the total international cooperation reports associated with legal entities during the examined period.

Analysis of the samples considered underlying incidents of the possible involvement of foreign legal persons associated with local entities (in line with the FATF's latest guidance on recommendation 24), as well as incidents of potential foreign politically exposed person (PEP) involvement. Furthermore, it considered when difficulty in identifying the ultimate beneficial owner was observed or a complex structure was employed to disguise the ultimate beneficial owner information. Of the total examined STRs/SARs, **28%** indicated the difficulty in fully identifying the ultimate beneficial owners (UBOs), and **7%** explicitly highlighted the employment of complex structures. These are in addition to the most frequent legal forms misused for possible illegal activities. Limited Liability Companies (LLCs) and Sole Establishments were the most frequent legal forms in the examined subject entities, accounting for **78%** and **13%**, respectively.

Moreover, **59%** of the examined entities were found to be incorporated on the Mainland, while **39%** were in Free Zones. The analysis also indicated other attributes such as the place (registrar) of registration, nationalities, and the most frequent business activities found in the sample of said STRs/SARs.

The following typologies and their associated risk indicators constitute the key findings of the analysis, wherein risk mitigation is required:

1. The possible abuse of legal persons as front or shell entities for illegal activities.
2. The possible abuse of offshore structures in illegal activities.
3. The abuse of legal persons in fraudulent activities.
4. The possible involvement of professional intermediaries (DNFBPs) in facilitating the abuse of legal persons in the UAE.
5. The possible abuse of legal persons for cross-border movement of funds.
6. The abuse of legal persons for conducting unlicensed hawaladar activities.
7. The abuse of legal persons in trade-based money laundering (TBML).
8. The possible abuse of legal persons to launder the proceeds of tax evasion.
9. The possible abuse of legal persons in proliferation financing.
10. The possible abuse of legal persons in sanction circumvention.

The above-indicated hypotheses were affirmed by examining the reviewed data and implied the possible misuse of local legal entities as a pass-through to route or layer unknown sources of funds. At the same time, the data did not affirm some hypotheses, such as the possible abuse of legal persons for human trafficking and terrorist financing as well as the possible abuse of legal arrangements and corporate vehicles by non-profit organizations (NPOs). This was due to the low volume of received STRs/SARs associated with these typologies. Nevertheless, the report underlined some observations; thus, the lack of findings on these patterns is not understood to be an absence of such illegal activities.

INTRODUCTION

Although legal persons[1] play a significant role in the global economy, corporate vehicles[2] have been misused in different illegal schemes and activities, including fraud, tax evasion, money laundering, and terrorist financing. In such cases, criminals and terrorists aim to disguise their identity and illegal proceeds by using corporate vehicles with complex legal structures across borders. In 2003, the Financial Action Task Force (FATF) strengthened its international standards for anti-money laundering and combating the financing of terrorism (AML/CFT) by stressing the importance of the identification and verification of beneficial ownership information.[3] Subsequently, in 2012, the FATF further developed its international standards to ensure the disclosure of beneficial owner[4] information and global transparency of legal persons and arrangements.[5] These were in addition to the Organization for Economic Cooperation and Development (OECD) international standards on beneficial ownership implementation.[6] Recently, the FATF revised its recommendations once again to ensure that "*there is adequate, accurate and up-to-date information on the beneficial ownership and control of legal persons that can be obtained or accessed rapidly and efficiently by competent authorities, through either a register of beneficial ownership or an alternative mechanism*."

In compliance with AML/CFT international standards, the UAE issued 'Federal Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations'[7] as well as Cabinet Decision No. (58) of 2020 Regulating the Beneficial Owner Procedures. These were in addition to Cabinet Decision No. (53) of 2021 Concerning the Administrative Penalties Against Violators of the Provisions of Cabinet Resolution No. (58) of 2020, as well as further guidance by supervisory authorities including the Ministry of Economy circulars and the Central Bank of the UAE (CBUAE) guidance for 'Licensed Financial Institutions Providing Services to Legal Persons and Arrangements.'

[1] The term 'legal persons' is used interchangeably with 'legal entities.' It refers to "any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, partnerships, or associations and other relevantly similar entities."

[2] Corporate vehicles refer to "companies, trusts, foundations, partnerships, and other types of legal persons and arrangements." FATF (2014) Guidance: Transparency and Beneficial Ownership, p.3

[3] FATF (2003) 40 Recommendations.

[4] Beneficial owner refers to "the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person. Only a natural person can be an ultimate beneficial owner, and more than one natural person can be the ultimate beneficial owner of a given legal person."

[5] FATF (2012) International Standards on Combating Money Laundering and the Financing of Terrorism, Recommendations 24 and 25.

[6] OECD (2019) Global Forum on Transparency and Exchange of Information for Tax Purposes: A Beneficial Ownership Implementation Toolkit.

[7] Including Federal Decree law No. (26) of 2021 to amend certain provisions of Federal Decree-law No. (20) of 2018, on anti-money laundering and combating the financing of terrorism and financing of illegal organisations.

While the UAEFIU issued its first strategic analysis typology report on the abuse of legal persons in 2021, this report expands the previously identified patterns to include different typologies and scenarios to develop the understanding of how corporate vehicles are potentially exploited and combined in illegal activities. This report is in line with the latest FATF guidance on Beneficial Ownership of Legal Persons (issued in March 2023), which requires identifying the most common typologies regarding the abuse of domestic legal persons and their possible nexus to foreign structures.[8] As such, this report underlines when it is relevant how the ultimate beneficial owner is disguised using different legal structures, intermediaries, and third parties. These include professional intermediaries such as legal and auditing firms, corporate service providers, consultancies, and management firms. Drawing on different hypotheses and the Legal Persons and Arrangements Risk Assessment, a number of frequently occurring risk indicators associated with the possible abuse of corporate vehicles are developed, including case examples.

OBJECTIVE

As part of the Strategic Analysis Plan (SAP) and in line with the UAEFIU's continual efforts to address and identify patterns of possible Money Laundering/Terrorist Financing (ML/TF) crimes, the UAEFIU is delivering its second report on the 'Possible Abuse of Legal Persons and Arrangements in Illicit Activities.'

This report intends to present the relevant outcomes from the strategic analysis based on the UAEFIU's broad range of data sources derived from stakeholders and reporting entities, and shall cover the following purposes:

- Extend the strategic analysis on the abuse of legal persons (LPs) in ML/TF, with consideration of a variety of hypotheses and scenarios.
- Identify new patterns and typologies pertaining to the abuse of LPs for ML/TF purposes.
- Develop risk indicators associated with identified patterns, subsequent to the previous risk indicators identified in 2021.
- Provide case examples underlining the major risk indicators.
- Promote the level of awareness and knowledge by sharing the outcome and conducting outreach sessions with the public and private sectors.

METHODOLOGY

The report illustrates possible patterns and typologies related to the abuse of legal persons from 1 January 2021 to 31 December 2022. The Research and Strategic Analysis Section (RSAS) draw different scenarios of typologies from the UAE National Risk Assessment, the Legal Persons and

[8] FATF (2023) Guidance on Beneficial Ownership for Legal Persons.

Arrangements Risk Assessment, as well as FATF publications, including published case studies by other jurisdictions. Thereafter, the RSAS proceed to test them, as illustrated in this report's subsequent parts. The developed scenarios and hypotheses comprise the following:

1. The possible abuse of legal persons as front or shell entities for illegal activities.
2. The possible abuse of offshore structures in illegal activities.
3. The possible abuse of legal arrangements in illegal activities.
4. The possible abuse of corporate vehicles by NPOs.
5. The possible abuse of legal persons for human trafficking purposes.
6. The abuse of legal persons in fraudulent activities.
7. The possible involvement of professional intermediaries (DNFBPs) in facilitating the abuse of legal persons in the UAE.
8. The possible abuse of legal persons for cross-border movement of funds.
9. The abuse of legal persons for conducting unlicensed hawaladar activities.
10. The abuse of legal persons in trade-based money laundering (TBML)
11. The possible abuse of legal persons to launder the proceeds of tax evasion.
12. The possible abuse of legal persons in terrorist financing.
13. The possible abuse of legal persons in proliferation financing.
14. The abuse of legal persons to evade sanctions or disguise the identity of a sanctioned person or entity.

This report's analysis illustrates whether the hypotheses prevailed and how LPs are being abused in the UAE. The data used are derived from available and accessible information within the UAEFIU's databases, particularly Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs). These are in addition to reports related to high-risk country activity (HRCA) that were received from registrars, as well as reports related to international cooperation (Inward Spontaneous Dissemination, Inward Requests for Information, Outward Spontaneous Dissemination, and Outward Requests for Information), along with other data and information obtained from domestic stakeholders, such as Law Enforcement Authorities including the Federal Authority for Identity, Citizenship, Customs and Port Security (ICP), Ministry of Economy (MOE), Ministry of Community Development (MOCD), Abu Dhabi Global Market (ADGM), Dubai International Financial Centre (DIFC), offshore registrars, among others.

The methodological process of data collection and analysis is explained in **Chart 1**

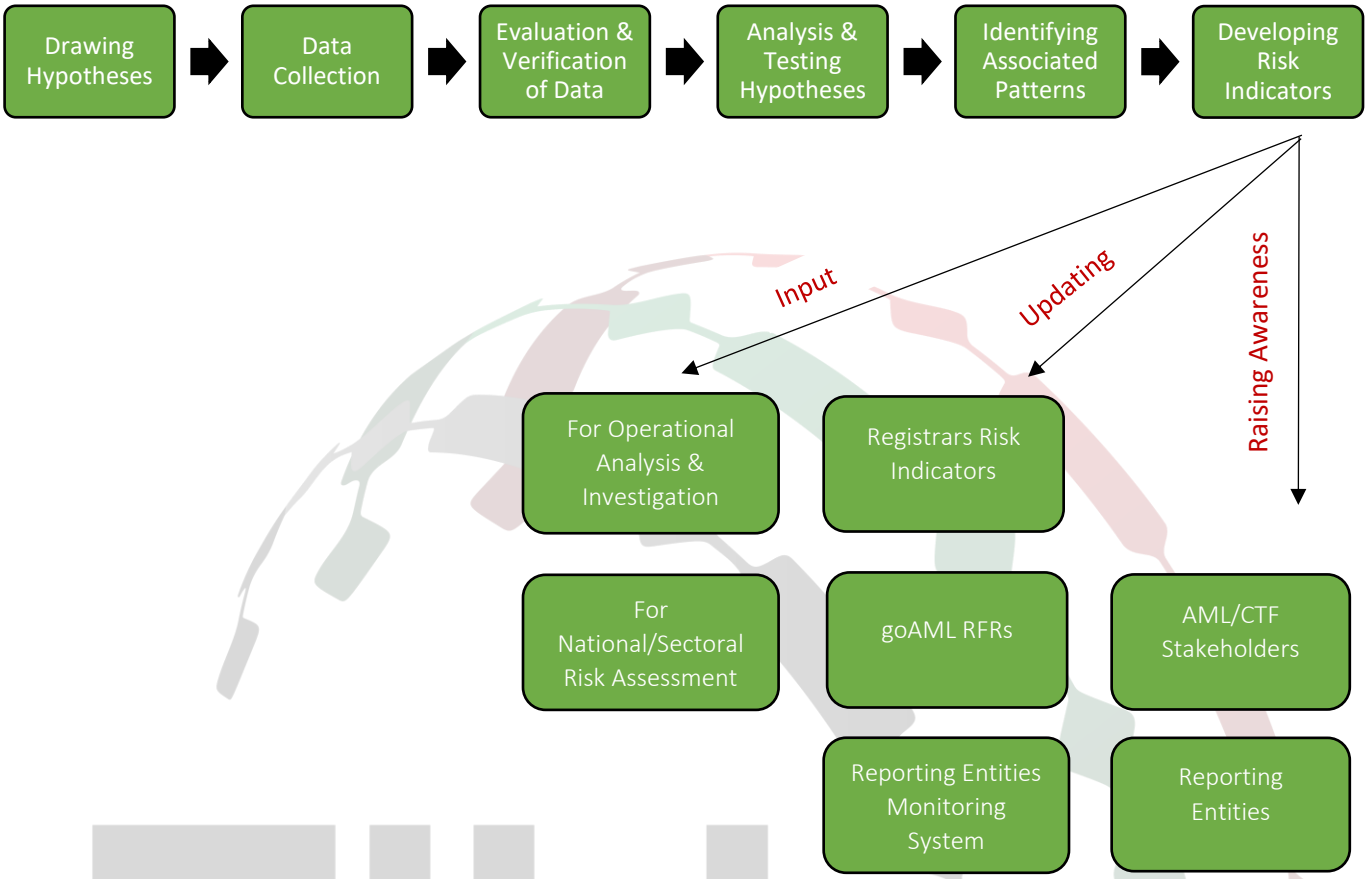


CHART 1 – *Strategic Analysis Methodology*

OVERVIEW OF RELEVANT DATA AND INFORMATION UNDERLYING THE ANALYSIS

This part provides insights into the collected data and information underlying this report's analysis, and implies different possible risk factors based on the outcome of the analysis. Some features, such as the nationalities of persons affiliated with the subject entities, the jurisdictions involved, and the types or forms of legal entities, were correlated with the criminal patterns and risk indicators identified in a later section of this report. The outcome of said data is summarized below:

1. Information and data received from the Ministry of Economy (MOE)

According to the information received from the MOE, the total number of registered entities in the UAE was **695,728** (as of the end of 2022), of which **75.4%** were registered on the Mainland and **24.6%** were registered in Free Zones.

Compared with the data previously collected by the UAEFIU in 2021, the number of registered entities increased between September 2021 and December 2022, with an overall increase of approximately **22.1%**. The majority of the increase was observed in the number of registered entities in **Financial Free Zones** (FFZs), constituting more than **224.6%**, followed by entities registered in **Commercial Free Zones** (CFZs) with an increase of **33.18%**, while the entities registered on the **Mainland** increased by **17.8%**.

CHART 2– *Percentage of legal entities established in the UAE, including their jurisdictions.*

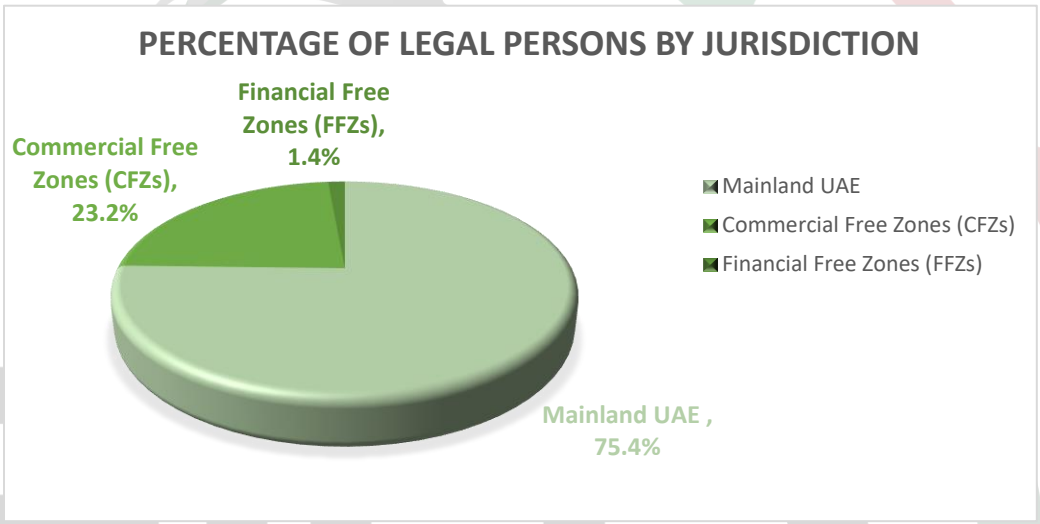
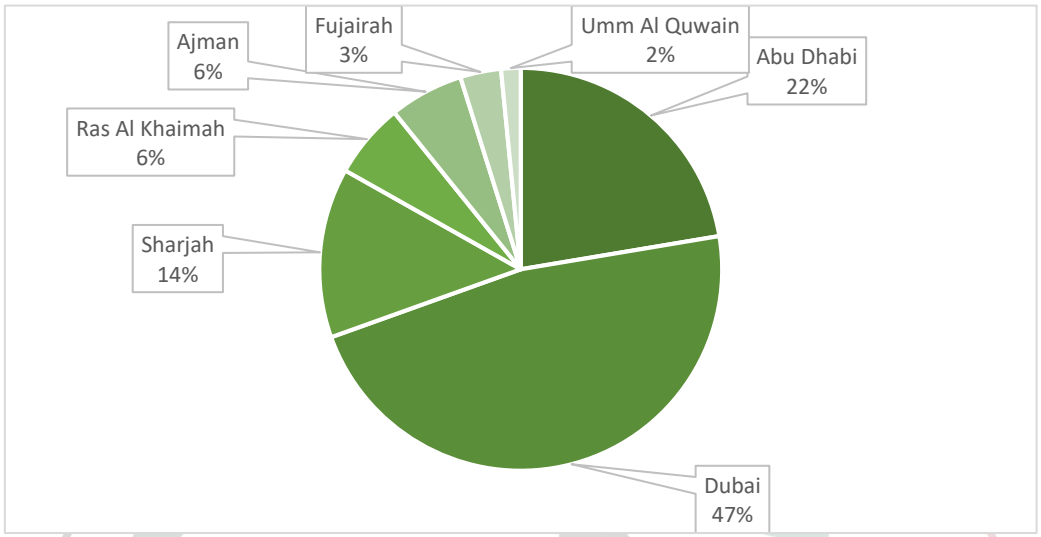


TABLE 1 - *Number of legal entities in the UAE by jurisdiction (as of December 2022)*

UAE Jurisdiction	Number of Legal Persons	Percentage (%)
Mainland UAE	524,667	75.4%
Commercial Free Zones (CFZs)	161,279	23.2%
Financial Free Zones (FFZs)	9,782	1.4%
TOTAL	695,728	100%

As indicated in the below chart, the majority of legal entities are established in Dubai and Abu Dhabi, followed by the other emirates.

CHART 3 – *Percentage of legal entities established in local emirates.*



During the examined period, as part of the MOE's supervisory role in the implementation of AML/CTF preventative measures related to legal entities and in improving the transparency of information related to ultimate beneficial owners, the MOE imposed **125 fines of AED 9.4 million**, **18 administration sanctions**, and **42 warnings on legal persons** that were found to violate/breach AML/CFT obligations.

2. Data and information relevant to legal arrangements and non-profit organizations (NPOs)

The UAEFIU has received limited suspicious reports in which the involvement of legal arrangements (i.e. trusts, foundations, asset or wealth management) has been established. In the UAE, legal arrangements are basically incorporated in the two Financial Free Zones, the **Abu Dhabi Global Market (ADGM)** and the **Dubai International Financial Centre (DIFC)**. These are in addition to the UAE Federal Decree-Law no. 19 of 2020 Concerning Trusts, regulating onshore trusts and establishing ownership rights over UAE onshore assets, particularly family-owned companies. It should be noted that the UAE Trust Law does not apply to trusts created in the ADGM and DIFC.

According to the information received from the **DIFC**, there were **293** registered **foundations** and **20 Company Service Providers** (**CSPs**) as of December 2022. The overall number of active companies under the DIFC was **4,377** (according to the DIFC website as of 13/03/2023). In the

DIFC, foundations can be set up for either charitable or non-charitable purposes (e.g., family succession planning) or to provide benefits to named persons. While trusts are used for asset protection, succession planning, and wealth preservation, in these arrangements the trustee (a DIFC company or a financial institution) will hold legal ownership of the trust property, while beneficial ownership remains with beneficiaries.

In the **ADGM**, foundations provide various functions, including wealth management and preservation, family succession planning, tax planning, asset protection and corporate structuring. Although foundations are similar to trusts, certain features are more akin to a company, such as being incorporated with a separate legal personality and holding assets in its own name on behalf of beneficiaries. According to the publicly available information of the 'Registration Authority' in the ADGM, a total of **184 foundations** were registered, of which **5 foundations** were '**Inactive'**, and **27** were '**Deregistered'** or '**Dissolved'**.

According to the FATF, an NPO is "a legal person or arrangement or organisation that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of good works."[9] In the UAE, an NPO is defined as "*any organized group, of a continuing nature set for a temporary or permanent time period, comprising natural or legal persons or not for profit legal arrangements for the purpose of collecting, receiving or disbursing funds for charitable, religious, cultural educational, social, communal or any other charitable activities.*"[10]

Similar to what was indicated previously, the UAEFIU received limited suspicious reports concerning the involvement of NPOs in illegal activities. At the same time, data received from the **Ministry of Community Development (MOCD)** indicated a total of **820 NPOs** registered in the UAE. The data showed that NPOs registered in the UAE are mainly licensed by the MOCD and the DIFC, followed by the Community Development Authority (CDA) in Dubai, the International Humanitarian City (IHC), ADGM, and Islamic Affairs and Charitable Activities Department (IACAD).

3. Relevant data and information related to 'Offshore' entities

Offshore entities are recognized as being inherently high-risk for ML/TF, according to the Legal Persons and Arrangements Risk Assessment. Offshore entities are found to be relatively easy to establish within the UAE as well as attractive to global investors because they are tax-exempt. The same was also observed in this report with different possible patterns related to the abuse

[9] FATF (2015) *Best Practices Paper on Combating the Abuse of Non-Profit Organisations*, p. 7

[10] *Federal Decree Law No. (26) of 2021 amending certain provisions of Law No. (20) of 2018, on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations*, p. 6

of offshore structures in suspicious activities. Both the Legal Persons and Arrangements Risk Assessment and the examined sample in this report underlined the offshore characteristic associated with foreign entities, which increase the difficulty of tracing or identifying the legitimate source of funds.

In the UAE, there are only **three authorities** that register '**Offshore'** entities— **Jebel Ali Free Zone (JAFZA)**, **Ajman Free Zone (AFZ)**, and **Ras Al Khaimah International Corporate Centre (RAK ICC)** with total number of **9379** registered offshore entities (as of December 2022). Generally, offshore entities are not issued with a business license but rather only a certificate of incorporation; this means that an offshore company cannot conduct any commercial activity within the UAE. However, RAK ICC allows investors to set up a corporate structure permitting offshore companies to carry out commercial activities in the emirate of Ras Al Khaimah by establishing subsidiaries with the **RAK Department of Economic Development (RAK DED)**.

4. Relevant data and information available with the UAEFIU database

Based on data extracted from the UAEFIU's reporting system **'goAML'** during the review period from **1 January 2021** to **31 December 2022**, the UAEFIU received **13910** out of 48416 Suspicious Transaction Reports (STRs)[11] involving legal entities in suspicious transactions. Out of said 13910 STRs, **6,461** were directly related to when a legal entity was involved as either a subject or a counterpart (be it as a sender or recipient or both). In addition, **1,694** out of 8503 Suspicious Activity Reports (SARs) were received during the same period in which a legal entity was involved as either a subject or a counterpart or both.

All reporting entities are required to select from a predefined list embedded in the reporting system at least one **'Reason for Reporting'** (RFR) that describes the primary concern(s) and the reason as to why the reporting entity is filing such a report to the UAEFIU. The following table demonstrates the top RFRs used by reporting entities in the received STRs and SARs involving legal entities.

TABLE 2 *– RFRs used by the reporting entities*

SN	Reason for Reporting	No. of Reports
1	Lack of appropriate documentation to support transactions.	2683
2	Transactional activity (credits and/or debits) inconsistent with a customer's alleged employment, business or expected activity, or where transactions lack a business or apparent lawful purpose.	1625

[11] This number excludes other types of suspicious reports such as HRC, HRCA, PNMR, and FFR.

3	Transactions that are inconsistent with the account's normal activity.	1166
4	Advance fee fraud/Phishing or email fraud/Inheritance fraud/fake prizes frauds/romance fraud	980
5	Account shows high velocity in the movement of funds, but maintains low beginning and ending daily balances.	775
6	No business rationale or economic justifications for the transactions.	740
7	The transaction is not economically justified considering the accountholder's business or profession.	568
8	An account that receives incoming electronic funds transfers then shortly afterward originates outgoing wire transfers or cash withdrawals slightly less than the incoming electronic fund transfers	373
9	Customer conducts several cash deposits in small amounts at ATMs.	320
10	Negative media reports or adverse news that the account holder is linked to alleged crimes or related to criminals.	223
11	No apparent business relationship between the parties and transactions.	211
12	Customer uses a personal account for business purposes.	202
13	FRAUD - Fund Recall Request	149
14	Funds deposited are moved quickly out of the account via payment methods inconsistent with the established purpose of the account.	138
15	Precious metals and stones (jewelry and watches included) transactions with non-resident individuals for cash transaction	138
16	Improper/incomplete file documentation, including borrower/buyer reluctance to provide more information and/or unfulfilled promises to provide more information.	129
17	Customer's home or business telephone is disconnected.	115
18	FRAUD - Fund Recall Request – International	107
19	A newly opened deposit account with an unusual amount of activity, such as account inquiries, or a large amounts or high number of incoming electronic fund transfers	97

According to the extracted data, the business activities of subject entities highlighted some concerns related to the sufficiency and availability of data filled by the reporting entities. As illustrated in (**TABLE 3**), the business activity most stated by REs was "**Unknown**" or "**Others**", which indicates that most reporting entities do not provide adequate or up-to-date information while reporting a suspicious report. Besides that, most businesses associated with reported LEs found to be related to '**Wholesale'** and '**Retail'** trading, '**Precious Metals and Stones**', '**Food and Beverages**', '**Construction'**, and '**Real-Estate**'.

TABLE 3 *– Business activities associated with the reported legal entities*

SR	Business Activity	Total No. of SRs
1	**Unknown** (Not specified by REs)	3156
2	Wholesale trade, except of motor vehicles and motorcycles	1207
3	Retail trade, except of motor vehicles and motorcycles	664
4	Wholesale of Jewelry, Diamond, and Precious Stones	393
5	Financial service activities, except insurance and pension funding	263
6	Food and beverage service activities	222
7	Wholesale and retail trade and repair of motor vehicles and motorcycles	209
8	Construction of buildings	171
9	Other professional, scientific and technical activities	151
10	Office administrative, office support and other business support activities	101
11	Manufacture of textiles	99
12	Other manufacturing	90
13	Real estate activities	88
14	Manufacture of computer, electronic and optical products	84
15	Computer programming, consultancy and related activities	80
16	Others	1671

Based on the analysis of reporting entities that submitted a STR or SAR against a legal entity as a subject or counterparty, **75%** of these STRs/SARs were received from **domestic banks**, **9%** from **foreign banks/representative offices** licensed by Central Bank of the UAE (CBUAE), **4%** from **dealers in precious metals and stones** (DPMS), and **4%** from **money exchange houses** licensed by CBUAE. The following table shows a breakdown of the reporting entity categories that have filed the STRs/SARs to the UAEFIU involving legal entities.

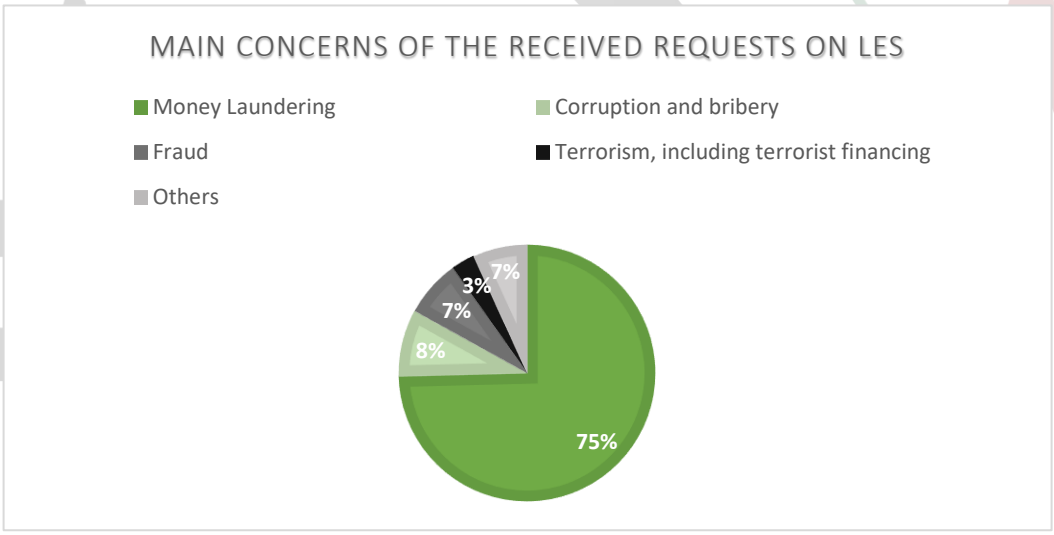
Ultimately, the UAEFIU disseminated a total of **202 cases** (a case may combine one or more suspicious reports) to Law Enforcement Authorities (LEAs) in which the subject(s) involved was an LE(s). As indicated in the table below, the cases related to LEs constituted approximately **57%** of the total disseminated cases.

TABLE 4 *– Number of dissemination against legal entities*

Year	Number of dissemination against LEs	% of dissemination against LEs compared with total disseminations
2021	90	62.9%
2022	112	53.1%
Total	**202**	**57.1%**

As for the data extracted from UAEFIU's **Integrated Enquiry Management System** 'IEMS', the UAEFIU received **7,267 requests** from domestic authorities such as **Ministry of Interior (MOI)**, **Federal Public Prosecution (FPP)** and **Law Enforcement Authorities (LEAs)**. The said requests were related to (database checks, name searches, freeze or unfreeze orders, or other types of information requests, among others). **1653** inquiries (approximately **22.7%**) of the received requests were related to legal entities, the majority of these requests were concerning the predicate offences illustrated in **Chart 4**.

CHART 4 – *Main concerns of the received requests on legal entities.*

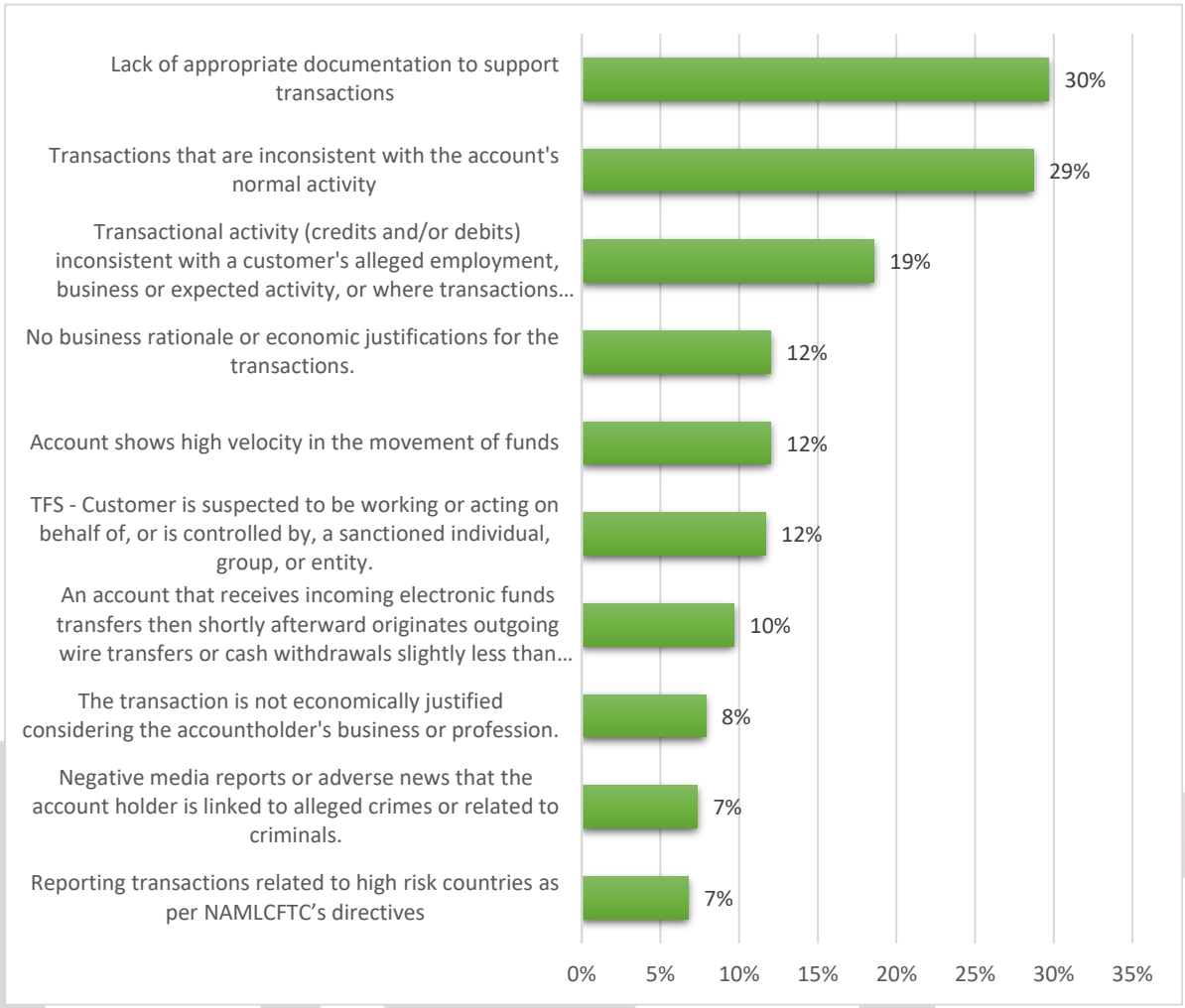


5. Reviewed sample of suspicious reports and intelligence reports exchanged with counterpart FIUs

Out of the total **8,155** suspicious reports (STRs and SARs) indicated previously that were linked to legal entities, **10%** were thoroughly examined for the purpose of this analysis (**705 STRs** and **114 SARs**). These were in addition to **80 High Risk Country Activity Reports** (HRCAs) received from different registrars.

From the review, most of the RFRs selected by the reporting entities were as presented in the following chart, which were found to be consistent with the overall RFR list in the data extracted from goAML.

CHART 5 – *The most frequent RFRs based on the reviewed sample.*



Moreover, the analysis indicated that **59%** of the involved entities examined were found to be incorporated **on the Mainland**, while **39% were in Free Zone jurisdictions**, with the remainder of 2% were in Financial Free Zones or unknown (the information could not be found in the suspicious report).

With regard to the legal form of said entities, almost **78%** were noted to be **Limited Liability Companies** (LLCs), followed by **13%** that were **Sole Establishments** and **5%** that were structured as **offshore** companies, as listed in **(TABLE 5)**.

TABLE 5 *– Legal form of examined legal entities*

Legal Form	No. of LEs	Percentage
Limited Liability Company	713	78%
Sole Establishment	114	13%
Offshore Company	46	5%
Private Company	10	1%
Civil Company	8	1%
Others	19	2%

Furthermore, the analysis underlined the most frequent business activities observed with the LEs involved in the reviewed sample. These activities included **general trading, trading in foodstuff, electronics, building and construction materials, and management and consultancy services**. These are in addition to petroleum/petrochemicals/oil trading and textile/garment trading.

The review has further highlighted some challenges in identifying or verifying the UBO information. As observed in the review, UBOs were perceived by reporting entities in some cases to be the shareholders or couldn't be identified due to the complexity of legal structure or involved transactions. Of the total reviewed suspicious reports, **28%** indicated the difficulty in fully identifying the ultimate beneficial owners. Still, intentional misrepresentation or hiding of the details of UBOs by the customer (or counterpart) cannot be ruled out. With regard to the complexity of ownership structures, it was recognized that **7%** of the entities involved in the reviewed sample have a complex ownership structure. Moreover, it was perceived that such structures were interrelated, with difficulty in identifying the beneficial owner(s).

Analysis of the samples considered underlying incidents of the possible involvement of foreign legal persons associated with local entities (in line with the FATF's latest guidance on recommendation 24), as well as incidents of potential involvement of foreign politically exposed persons (PEPs). The percentage of PEP involvement identified in the analyzed sample of

STRs/SARs was **2%.** Furthermore, the analysis highlighted some jurisdictions of concern in which they incorporate foreign entities found to be associated with subject local legal persons.

Ultimately, international requests were also considered and reviewed to enrich the analysis outcome. From 1 January 2021 until 31 December 2022, the UAEFIU received **961** Inward **Requests for Information** (IRFIs) and **222 Inward Spontaneous Disseminations** (ISDs) comprising concerns related to legal entities as a subject or counterpart. During the same period, the UAEFIU sent to other counterpart FIUs **251 Outward Requests for Information** (ORFIs) and **136 Outward Spontaneous Disseminations** (OSDs) related to legal entities as a subject or counterpart. The exchanged intelligence reports related to legal persons represent around **57%** of overall received/sent requests and information.

The RSAS has reviewed **10%** of the overall **1570** reports sent/received to/from counterpart FIUs to test the hypotheses initially set at the beginning of this strategic analysis (i.e. possible TBML, laundering the proceeds of tax evasion, possible ML through shell companies, among others). The findings were combined with the identified patterns later in this report.

6. Review of 'Cash Declaration' records from Federal Authority for Identity, Citizenship, Customs and Port Security (ICP)

For the purpose of assessing the volume of funds entering or exiting the UAE on behalf of legal entities, the UAEFIU performed a review of cash declaration records during the period from 1 January 2021 until 31 December 2022 in which 'specific purpose' was related to legal entities. The review indicated **16,374** 'incoming' cash declarations as well as **2,833** 'outgoing' cash declarations.

Furthermore, the most frequent purposes indicated for cash arrivals were '**Purchase of goods**', '**Exchange**', which were mainly by Limited Liability Company (LLCs).

During the examined period, the top that arrived in/departed from the UAE were US dollar (**USD)**, Saudi Riyal (**SAR)**, Euro (**EUR)** and **AED**.

IDENTIFIED TYPOLOGIES AND PATTERNS

This section provides an overview of the identified typologies and patterns related to the possible abuse of Legal persons and arrangements in illegal activities. Some of these patterns are emerging techniques noted in recent suspicious reports, while others have been previously identified and continually observed in different strategic analysis projects. According to the outcome of the analysis, not all considered hypotheses (as stated in Methodology) were corroborated due to data limitations in some aspects.

1. The possible abuse of legal persons as front or shell entities in illegal activities

The involvement of shell or front entities was considerably observed in most of the tested hypotheses in this analysis report, since they are prevalent in ML/TF schemes. The observed pattern starts by establishing an entity and using its multiple bank accounts to move funds through financial institutions (FIs) in the UAE. The funds are subsequently routed through different counterparties and moved from the source via multiple layers of transactions, both domestically and internationally. The accounts were found to be funded by high inward remittances and transfers, cash deposits, or cheque deposits, followed by immediate outward remittances directly or indirectly involving different counterparties and foreign entities. It was noted that different entities involved in the examined sample were found to have no physical appearance, whether based on FIs' inspection visits or the entity did not show any business expenses (Shell Company). These were in addition to entities that were found to be operating as a Front Company, including flexi or smart desks; for example, approximately 3% of entities involved in the examined sample were registered as a 'Flexi-desk'.

Most of the shell or front entities are suspected of concealing the proceeds of illicit activities by funding business activities, commingling illicit proceeds with legitimate business proceeds (in the case of front entities), or purchasing assets, obtaining debt facilities and then paying them off under the name of the entity (as in shell entities) to hide the details of the UBO. Another observation noted is the rapid financial growth of a newly established company, with a business nature that is not expected to have a large amount of inflow and outflow of funds in a short period of time, or when the entity's owner is perceived to have no business background and seems to be unfamiliar with the established entity's business activities.

TBML techniques are also commonly used by shell and front entities to move funds disguised as trade transactions through creating false or multiple invoices, ghost shipping, and over- and under-invoicing. Legal persons were also observed to be transacting with counterparties in a

different line of business, e.g., a food and beverage trading entity trading with a machinery and raw materials heavy equipment trading company.

Finally, involved entities in different incidents were found to have a nexus with possible sanctioned individuals or entities or have ties to criminal groups. Such links were established based on name screening or derogatory remarks in media reports or open sources.

2. The possible abuse of 'offshore' structures in illegal activities

The sample examined in this report indicated the misuse of offshore companies' structure as a vehicle to move suspicious funds, TBML, as well as purchasing of assets on behalf of third parties or criminal networks. The reported STRs/SARs illustrated that subject offshore companies mainly intended to conceal a beneficial owner(s) subject to sanction or involved in the proliferation of terrorism, drug trafficking, or defrauding and scams/Ponzi schemes abroad, as well as foreign PEPs linked to alleged corruption or predicate offenses prosecuted abroad. The analysis of said suspicious reports also underlined a complex legal structure and reporting entities' difficulty in identifying the ultimate beneficiary in several incidents.

One of the patterns observed in this typology is for a registered owner(s) to act as a director for different offshore companies and other local legal entities (Limited Liability Companies) in the Free Zone. In one unique incident, for example, 10 offshore companies were associated with three other Limited Liability Companies (LLCs) established in Free Zones that were registered under the same reported owner and other family members. In such an incident, it was found that a family member was involved in large-scale drug trafficking activities in a foreign jurisdiction. His/her shareholding of investment was transferred to the registered owner of different offshore companies in the UAE (as legal heirs).

Said pattern is combined with using the legal entity's bank account to move funds through inward remittances (followed by immediate cross-border wire transfers) to different locations and foreign counterparties. Ultimately, the legitimate origin of the funds, the relationship with counterparties, the purpose, and the economic rationale behind the transactions of the funds could not be ascertained.

3. The possible abuse of legal arrangements and nominees in illegal activities

The UAEFIU received few STRs/SARs directly or indirectly involving some legal arrangements (such as trusts, foundations, asset and wealth management, and investment arrangements). The low volume of data obscured reaching a conclusion or identifying a specific pattern related to the abuse of legal arrangements in the UAE. However, an examination of the received suspicious reports indicated that some attempts at possible illegal activities through establishing legal

arrangements were made by a branch of a foreign company, a foreign private limited company, or a subsidiary of a public joint stock company. These were in addition to potential owners who approached a corporate service provider(s), auditor(s), or legal advisor(s) about establishing legal arrangements that were not supported by the required minimum customer due diligence (CDD) documents, as well as a potential owner(s) who was linked to adverse media, a possible sanction breach, or a high-risk country (including offshore centers). These were in addition to high-profile customers posing an increased risk of corruption. The term 'potential owner' here is used to refer to neither transactions nor arrangements being proceeded, as well as new customers being denied the obtainment of such a service based on the reporting entity's screening results and risk monitoring procedures. Some of the reported suspicious activities indicated the involvement of nominee directors with trusts as shareholders. In other incidents, the legal structure was complex, the identification of shareholders was obscured, or the ultimate beneficiary in a foreign jurisdiction was unnamed (e.g., the ultimate beneficiary of charities).

4. The possible abuse of corporate vehicles by NPOs

The UAE has strong licensing and financial controls concerning NPOs, combined with adequate monitoring by supervisors to prevent their abuse. The UAEFIU received few STRs/SARs directly or indirectly, indicating the abuse of local NPOs in illegal activities. As such, reaching a clear pattern relating to NPOs was unfeasible, but some possible techniques were noted during the sample review. The first method involves foreign NPOs routing funds to the UAE through different legal person accounts. The foreign NPO remitter is suspected of funding terrorist organizations or having links to TF activities, as per public domain searches/available databases. Another red flag that could be considered is when a legal entity receives funds from some foreign NPOs for humanitarian-related activities and subsequently transfers a portion of the funds to a third party (an individual or another legal person) without sufficient justification. Another observation was related to suspicions when the beneficial owner of a local entity (NPO) is found to be the owner of other legal entities that have been the subject of suspicious reports filed to the UAEFIU. These are in addition to when a legal entity (NPO) conducts transactions with other local entities not in line with its KYC profile.

As an additional observation, a local NPO approaches a reporting entity (a financial institution) and states that there will be an incoming transaction related to the NPO's activities for a specific purpose. The NPO tries to gauge whether the RE is comfortable with the transaction mentioned, while the RE's raising of questions will mostly result in the anticipated transaction not being materialized. When an RE performs additional information collection (including public domain), transactions appears inconsistent with the foreign donor and related parties' known profiles (according to public domain).

5. The possible abuse of legal entities in human trafficking

The UAE condemns, prohibits and penalizes human trafficking and aims to fight it both regionally and abroad. Human trafficking involves all forms of violence, including domestic violence, sensual exploitation and forced labor. No patterns were identified from the few STRs that the UAEFIU received during the review period. However, some observed methods were found to involve legal entities established in the UAE, which might be receiving funds linked to human trafficking abroad.

As observed from the received STRs/SARs, LE accounts received funds from individuals or other LE accounts abroad; the funds were suspected to be proceeds of 'false recruitment' or the issuance of work permits to assist in the illegal migration of individuals from their countries (prominently high-risk countries). The entities involved were in 'consulting & employment,' 'tourism,' and 'technical works.' In another observation, the beneficial owner of a legal entity was linked with media reports and derogatory remarks about being involved in money laundering, tax evasion, human trafficking, fraud and forgery. However, there was not sufficient information to understand whether or not and how the LE was being abused in human trafficking.

6. The abuse of legal entities in fraudulent activities

Analysis of the sample reviewed implies that criminals tend to abuse legal entities' accounts to move fraudulently derived proceeds through electronic transfers or physical cash movements (cash couriers declaring on behalf of LEs). In most scenarios, the original fraudulent activity occurs in a foreign country, of which the proceeds are routed to the UAE, particularly to accounts held by legal entities. Said accounts are either controlled by the fraudsters directly or their allies or controlled by gatekeepers in more sophisticated fraud operations (as Company Service Providers 'CSPs'). Such schemes might involve a complex network of various shell companies operating in the same jurisdictions or extending to some other jurisdictions, interacting with one another through purportedly legitimate transactions such as service fees, own-account transfers, or debt payoffs.

For example, with regard to a CSP controlling an LE, the UAEFIU received a STR in which the reporting entity was the victim of fraud. In this case, a Special Purpose Vehicle (SPV) opened a corporate bank account with the RE, obtained a mortgage loan based on the misrepresentation and omission of critical information by colluding with the seller (a legal entity), and provided false information as part of the mortgage loan application submitted to the bank, which is material in nature and against which the lending was granted.

In other reviewed STRs/SARs, the types of entities found to be mainly involved were 'LLCs' and 'sole establishments' incorporated primarily on the Mainland. The business activities of the entities involved were mainly 'general trading' and 'marketing' or 'consultancy.' The most repetitive pattern involves 'investment fraud' and using the accounts of LEs to receive funds from prospective investors and then routing the funds through multiple LE accounts. In this pattern, the entity is registered as a general trading company, opens a bank account, and immediately starts receiving multiple payments referred to as 'investments,' 'financial services,' or 'personal investments.' The funds are subsequently transferred to other LE accounts, allegedly toward business-related entities/counterparties. The transactions are substantiated by 'clearly' false documents and agreements, whereby indicating possible investment fraud and, more likely, a 'Ponzi scheme.' Because of that, some entities use misleading and deceptive names similar to those of popular establishments to gain the victim's trust and defraud them.

In very few reports, the involvement of 'crypto wallet development businesses' and other similar activities was also observed to be tied with an identified emerging pattern involving entities promoting crypto investments and misleading victims to invest in the digital currency products that they offered, which had on some occasions no monetary value. The pattern involves multiple entities in different jurisdictions, and in this context, the UAEFIU has also received intelligence reports from counterpart FIUs on similar concerns (e.g., virtual currency Ponzi scheme).

Another popular scheme found is the use of social media and online trading platforms to dupe prospective buyers (victims) into purchasing high-value goods and items like luxury brands and gold; after the payment is processed and received by the LE account, the buyer receives no actual goods. On the other hand, multiple gold and jewelry entities were found to be involved in layering possible fraudulent proceeds from ill-gotten (stolen) gold that was imported from outside of the UAE by other jewelry entities; the payments were not received by the exporters (who, as informed by the RE, filed complaints with the relevant LEAs in their country), and the possible proceeds from selling this gold were routed through multiple entities' accounts in the UAE.

7. The possible involvement of professional intermediaries (DNFBPs) in facilitating the abuse of legal persons in the UAE.

Designated Non-Financial Businesses and Professions (DNFBPs) are subject to AML/CTF obligations and the application of preventative measures such as conducting customer due diligence, the identification of beneficial owners, and reporting suspicious ML/TF activities. Nevertheless, a sample of STRs/SARs examined for the purpose of this report indicated possible misuse of legal entity structures in the UAE by DNFBPs to intentionally disguise the identity of a UBO(s) or source of funds potentially related to money laundering, fraud, tax evasion, and avoiding sanctions, among others. Said sample focused on the possible involvement of DNFBPs

such as legal and auditing firms, management and consultancy firms, real estate agents, and corporate service providers (CSPs), while excluding dealers in precious metals and stones (DPMS) because the UAEFIU dedicated a full strategic analysis report concerning the abuse of DPMS for ML purposes, which was published in September 2022.

Analysis of the purposive sample illustrated that the most frequent legal forms employed by DNFBPs in the reported suspicious activities were 'sole establishments' and 'Limited Liability Companies,' followed by 'offshore' companies, be they on the Mainland or in the Free Zone, but also where they were licensed as a 'flexi-desk.' The majority of these reported DNFBPs were newly established. In different incidents, it was noted that the entity's activities on the 'Know your Customer' (KYC) document differed from trade licenses and other businesses that could be combined under the same code of activities. For example, a transaction involves the trade of real estate assets by an entity licensed for 'foodstuff catering' and 'event management,' or the engagement of unlicensed (remittance) activities by a DNFBP. Moreover, some of the DNFBPs, such as management consultancies, were found to transact in significantly high-volume amounts through providing tourism and lifestyle services, even amidst the global pandemic restrictions. While the beneficial owners were identified in most incidents, several STRs/SARs underlined the difficulty in identifying the ultimate beneficial owners and the involvement of multiple shareholders and signatories or third parties.

The commonly recognized pattern identified through the analysis is the abuse of DNFBPs as a vehicle through which to conduct transactions on behalf of third parties abroad and/or for the layering of funds in the UAE. This is done through DNFBPs receiving multiple incoming wire transfers and conducting structured cash deposits or using clearing cheque deposits, followed by immediate outgoing fund transfers, cash withdrawals, and outgoing cross-border payments. These transactions involved different counterparties abroad receiving or sending transfers, while these counterparties were not disclosed in the KYC, and the DNFBP failed to provide genuine documents with which to substantiate its relationship with them. Such a pattern noted in most STRs led to the conclusion that the UAE is used as a pass-through to route or layer unknown sources of funds. In different cases, the DNFBP's personal account was also used to receive a high value of inward remittances from the same third parties. This further suggested the DNFBP's involvement as a facilitator or professional money launderer for fund movements. In addition, there were no operational expenses observed in the reported DNFBP's accounts or audit reports that would support the existence of an actual business.

In a few STRs, it was noted that the company's contact information (e.g., contact number or company website) was in another country (despite operating in the UAE). Moreover, adverse media found different counterparties involved in the examined STRs/SARs to be foreign

fraudsters, drug traffickers, PEPs, and sanction-related concerns, or subjects of other jurisdictions' criminal procedures. These were in addition to receiving different enquiries from correspondent banks on the DNFBP's transactions, as supported by the earlier conclusion. Ultimately, a few STRs suggested that funds eventually ended up in the real estate sector abroad. However, there were no sufficient data with which to support this finding as a related pattern.

The second identified pattern in this typology combines trade-based money laundering (TBML) techniques with the previously explained one, such as phantom shipments, invoice fabrications, the absence of an invoice number or a description of goods (quantity and unit price) and payment terms, as well as providing multiple contrasting draft copies of bills of lading. These include DNFBPs' inability to share transport documents with which to ascertain the trading activity and movement of goods with counterparties, as they have claimed to financial institutions. As such, the most frequent reason for reporting indicated in this typology was the lack of appropriate documentation with which to support transactions.

Ultimately, despite the thorough examination by the RSAS as well as information provided by financial institutions in their STRs/SARs, the legitimacy of funds placed in DNFBPs' accounts and the ultimate usage could not be ascertained. Additionally, it is worth highlighting that the number of cash-related transactions and the cash volume noted in the reported STRs/SARs raise concern more than do the non-cash transactions, since it is expected that DNFBPs, such as consultancy and legal firms and corporate service providers, could conduct most of their local business transactions through electronic or wire transactions. Another matter of concern lies in dealing with high-risk countries and possible sanction breaches. In some STRs, shipment documentation used by the subjects of the STRs (DNFBPs) in supporting their claims indicated that shipments were to arrive in a sanctioned/high-risk jurisdiction, not in the UAE (as claimed). Such cases further establish the possible abuse of DNFBPs in sanction circumvention.

8. The possible abuse of legal entities for cross-border movement of funds

Previous strategic analysis reports issued in 2021 and 2022 indicated two patterns concerning the possible abuse of LEs and Money Service Businesses (MSBs) in cross-border movement of funds. The same patterns were continuing to be observed as when LEs are being abused by MSBs for cash border movement and transportation in particular. This starts with several individuals of high-risk nationalities arriving from different high-risk jurisdictions while carrying cash in various currencies to the UAE. This cash is declared to the local customs authority in favor of an LE or MSB. The findings suggested that there could be a couple of possible scenarios for this, including: (1) Funds' beneficiary LE is only a front/shell company whose role is to receive funds on behalf of

an MSB to avoid documentation; (2) Funds are directly declared for an MSB which is possibly conniving with a third party to launder proceeds of crime.

The latter pattern occurs when a DPMS entity is possibly involved in gold smuggling from conflict/affected high-risk areas or in the illegal transport of gold through another high-risk jurisdiction. The smuggled gold is further sold to local DPMS entities or processed and re-exported to Western European countries.

In the review of the sample, some observations were noted in which a UAE legal entity could act as a party or an intermediary in the possible smuggling of goods in a foreign jurisdiction and/or a transit jurisdiction of illegal proceeds, e.g., a legal entity supplying (restricted) goods to a foreign distributor, who then exports the same goods to a neighboring country and smuggles them back to the foreign distributor. Besides this, several cross-border payments were noted between the involved UAE entity and the foreign distributor. Another example is when a UAE bank account is being abused to siphon funds from the country in which the original crime occurred (as a pass-through account). Proceeds are then routed out of the country to further layer/distance it from the original actors, or are utilized as capital to invest in a business or high-value assets within the UAE.

9. The abuse of legal entities for conducting unlicensed hawala activities

In different cases, the analysis indicated that legal entities were suspected to be engaging in unlicensed/unregistered hawala (UHP) activities with the absence of a 'Hawala Provider Certificate' granted by the Central Bank of the UAE (CBUAE) in addition to their primary commercial/business activities being licensed by other licensing authorities. UHPs tend to commingle funds specific to illegal hawala activities with usual funds resulting from regular business activities (legal entities are used as front companies).

On the other hand, LEs, be they Registered or Unregistered Hawala Providers (RHPs/UHPs), were found to be directly involved in the physical transportation of a large amount of cash (cross-border cash movement) in different currencies. LEs would use groups of cash couriers to transport cash through multiple jurisdictions on their behalf. In different incidents, the cash was declared under the name of the LE or the hawala provider (in the case that the LE was an RHP). In other cases, couriers might not have declared that the cash was related to the LE or RHP. However, the cash movement would indicate being intended for net settlement or cover payments.

The entities involved in said patterns were mainly in the business of 'general trading,' 'foodstuff,' or 'dealers in precious metals and stones' and were primarily found to be established as LLCs and incorporated in mainland jurisdictions.

10. The abuse of legal entities in trade-based money laundering (TBML)

The identified patterns in this typology were consistent with those previously identified in the UAEFIU typology report on trade-based money laundering (TBML) in 2021. TBML mainly involves exploiting the trading system to obscure the true origins of illicit funds. TBML schemes vary in complexity, but typically involve misrepresenting the price, quality and quantity of goods/services. Such exploitation is tied to the abuse of legal entities by organized criminal groups, professional money launderers, and terrorist financing networks (also known as trade-based terrorist financing).

Analysis of the reviewed sample indicated that the main TBML techniques involving legal entities included: (1) False reporting/description on invoices, such as commodity misclassification; (2) Commodities traded not matching the profile of the LE's business activity; (3) Obvious use of shell companies or offshore front companies; (4) Third party intermediaries facilitating the transaction or invoice settlements; (5) Abuse of the existing trading chain to move funds, possibly related to the evasion of sanctions/financing of terrorism.

It was also observed that legal entities involved in TBML had complex ownership structures, with local entities collaborating with foreign ones (e.g., holding companies). In such a case, the legal entity in the UAE receives multiple wire transfers from a legal entity in a foreign jurisdiction shortly after funds have been moved to a third jurisdiction or transferred to a local legal entity. Furthermore, it was noted in different instances that the name of the recipient entity was similar to the name of the initial originator of funds, which could possibly indicate the possible abuse of LEs in the UAE to bypass/receive funds related to tax evasion, among others, through the use of TBML techniques.

11. The possible abuse of legal entities to launder the proceeds of tax evasion

The reviewed sample implied that most LEs being misused in the UAE for possible tax evasion purposes are established in Free Zone jurisdictions and licensed to provide consultancy and advisory services. It was also noted that adverse news related to tax evasion cases in another jurisdiction usually triggers local REs' suspicious reports on a legal entity for possible laundering of the proceeds of tax evasion.

One of the common patterns observed through examining international reports received by the UAEFIU underlined using trade-based techniques for tax evasion and laundering its proceeds. Such techniques included legal entities importing or exporting goods using under-invoicing to intentionally manipulate the price of the goods (as opposed to their market value) so as to pay lower tax duties. The pattern could also be combined with routing funds through shell companies to disrupt the money trail.

Another significant pattern noted through the review of international reports involves various predicate offenses and ML schemes, including using front or shell companies, trade-based techniques, fraudulent activities, and tax evasion. Such a pattern is commonly known as "VAT Carousel Fraud" or "Missing Trader Fraud",[12] which is essentially a type of VAT fraud that attempts to exploit a jurisdiction's VAT rules through indirect series of repeated trade-based transactions and activities. In such a case, a local legal entity is suspected of being misused as a passage to launder illicit proceeds from the aforementioned fraud type. Initially, products are sold to foreign shell companies without charging VAT as a movement of goods within the same territory. These shell companies will then sell the same goods to another company charging VAT. The transfer of value and goods will proceed until the "missing trader" does not pay the due VAT to the government, regardless of whether the buyer was charged. Although the tax was not paid, the original seller of products will file a VAT claim against the sale of goods, creating a two-fold loss to the government.

12. The abuse of legal entities in possible terrorist financing (TF)

Due to the few available STRs/SARs reported to the UAEFIU concerning misusing local legal entities for terrorist financing purposes, identifying patterns related to this typology was unfeasible. Moreover, most of the reported STRs/SARs were found to be more related to possible sanction breaches than to straightforward terrorist financing. However, some observations were noted concerning the possible smuggling of goods, e.g., cigarettes, wherein the profit from smuggled goods would potentially be used in funding a designated terrorist group. Other observations were related to a few suspicious transactions routed through UAE trading entities or counterparties to possible designated parent entities of terrorist groups overseas, using entities' bank accounts, exchange houses, and registered and unregistered hawaladars. The licensed activities of such suspected entities included a variety of trading businesses, such as general trading, foodstuff, and electronics, as well as DPMS and real estate brokerage firms. Still, the ultimate remitter or beneficiary in the noted incidents and the exact purpose of receiving

[12] FATF GAFI (2007) Laundering the Proceeds of VAT Carousel Fraud.

funds were often unclear. Ultimately, such incidents were reported to state security for investigation.

13. The possible abuse of legal entities in proliferation financing (PF)

In this typology, despite the few suspicious transactions and activities reported to the UAEFIU in relation to the possible abuse of legal entities in proliferation financing, the quality of reported data in addition to the in-depth analysis conducted on these reports indicated different primary patterns. The analysis illustrated that most legal entities identified as a subject of STRs/SARs related to PF suspicion were mainly established as limited liability companies, with few being established as sole establishments or private companies, whether on the Mainland or in Free Zones. However, many of these entities were also found to have a link to or could be (informally) a branch of a foreign company or an offshore (Ltd.) company set up in a high-risk country. The most dominant business activity noted in entities' trade licenses was 'general trading' of different types of goods, including foodstuff, electronics, building and construction, and jewelry, as well as trading in refined oil (the material in petroleum and chemicals). Nevertheless, it was also noted that the business activity indicated in the legal entity's trade license or KYC was not necessarily consistent with its actual line of business. For example, an entity's trade license would involve activities such as 'sea cargo services,' but an examination of the entity's transactions and supporting documents would indicate the company to be facilitating the movement and transfer of funds (or acting as a hawaladar) between a buyer and seller, which is not permitted because the company is not certified to do so.

Goods involved in said STRs/SARs included possible dual-use and high-risk goods such as chemicals, petrochemicals, oilfield chemicals, medical and surgical articles, radioactive materials, and trading in high-end unmanned aerial vehicles (drones), among others. These were in addition to importing devices or badges which can detect radioactive materials while transporting said materials. Still, in all reported STRs/SARs, legal entities were reluctant or refused to provide complete information on the goods that they were exporting. As such, the most frequent reason for a PF suspicion being reported by financial institutions and insurance companies was mainly related to "a customer or transaction that is suspiciously involved in the supply, sale, delivery, export, or purchase of dual use, controlled, or military goods to countries of proliferation concerns." The majority of reported suspicious activities involved high-risk countries or transactions related to shipment routes through countries with weak export control laws or weak enforcement of export control laws.

In different SARs, the nationality of the beneficial owner was the same as the destination or the route used in the scheme. Some SARs indicated that the beneficial owner had been subject to other STRs/SARs or criminal procedures in other jurisdictions. On the other hand, analysis

illustrated the difficulty in identifying the ultimate beneficial owner (UBO) of the company and company account due to using an unnecessarily complex transaction structure or non-disclosure of the source of funds. Within this context, a pattern was noted concerning the involvement of multiple individuals as beneficiaries, shareholders (e.g., four to five shareholders) with different directors, and multiple authorized signatories in a structured, complex setup that obscures reaching the UBO. Such a structure also included frequent changes in ownership, which further suggests the intention to conceal the UBO and the origin of funds.

Aside from the following indicated typology in this report in relation to sanction evasion and its strong association found with the proliferation of financing in many circumstances, the analysis underlined that local legal entities could also be misused as intermediaries or front companies for third parties associated with possible PF. The transaction pattern noted comprises receiving electronic or wire transfers and remittances related to the supply of goods to high-risk countries. These transfers involved domestic and cross-border logistics companies and management firms, or transfers from frequent third parties to legal entities' bank accounts and beneficial owners' personal accounts. Rapid movement of funds was also noted through cash as well as inward and outward remittances for trade activities conducted through a third port of shipment involving high-risk jurisdictions. No business-related expenses were noted in the company account, such as salaries or other business expenses.

Another identified pattern found to be associated with the previous transaction pattern is the utilization of TBML techniques. The majority of suspected transactions were related to goods bought or sold. At the same time, the subject legal entity had failed or refused to substantiate their shipment/port documents, bill of lading, certificate of origin, onboarding booklet, and information on the origin of the goods or the source of funds. TBML techniques included fabricating invoices, undervalued shipments, routing multiple destinations with no apparent business or commercial purpose, discrepancies in the description of goods or commodities on the invoice or in the actual goods shipped, and missing quantity, unit and packing details. These were in addition to the fabrication of a different date of shipment from the one indicated in the bill of lading. Overall, incomplete file documentation, ambiguous transaction details, and unknown end users were noted.

14. The possible abuse of legal entities in sanction circumvention

Analysis indicated the possible abuse of legal entities as a vehicle through which to route transactions on behalf of a sanctioned entity or third party. Most legal entities reported to the UAEFIU for potential sanction evasion were Limited Liability Companies (LLCs) established in Free Zones and also on the Mainland, particularly Dubai, practicing various codes of activity, but mainly general trading of different goods and items, as well as consultancy firms. Within this

context, it was noted that different legal entities were established in both the UAE and in sanctioned jurisdictions to facilitate the movement of funds.

Most of these reports were related to international sanction regimes, followed by jurisdictions' national sanction lists. Many of these suspicious reports indicated the possible intent to form a legal entity through multiple beneficiaries and shareholders while involving several authorized signatories as a complex setup to disguise the UBO. Furthermore, it was noted that not only newly established entities were the subject of reported suspicious activities, but also entities that had been subject to multiple changes in shareholders, directors, and business activities. Considering the nationalities and jurisdictions involved, this change in ownership structure suggests an attempt to conceal information on an ultimate beneficial owner who is subject to sanctions or a national of a sanctioned or high-risk jurisdiction. At the same time, multiple SARs reported by local registrars in Free Zones were identified as potential owners, as the subject was an individual who had failed to obtain a trade license due to the registrar screening process in identifying the subject as a possible sanction offender.

This typology's commonly observed transaction pattern is the rapid movement of funds as well as excessive layering of transactions by the account owner through different local bank accounts. This is in addition to routing payments made toward entities with links to a sanctioned individual or jurisdiction. Moreover, this pattern was also combined with TBML techniques, including fictitious trade transactions and misrepresenting shipment documents to obscure vessels' actual destinations or routes so as to circumvent sanctions. Ultimately, local legal entities are likely used as a front or a pass-through route on behalf of a sanctioned individual or entity.

Another observation exhibiting the abuse of LEs for sanction evasion purposes is when an LE is set up as a front company to route transactions on behalf of a sanctioned entity. These funds are disguised as payment against fictitious commercial transactions. This is a typical technique employed when an LE has a presence in both the UAE and a sanctioned jurisdiction. In this way, the LE in the UAE can ease the process of sending or receiving funds in favor of the (group) entity in a sanctioned jurisdiction. Affiliation with sanctioned entities or countries can sometimes be verifiable through a public domain search or by means of a thorough investigation by the RE and concerned authorities. When suspicion has been raised against a particular entity, there is also a tendency that the LE will undergo a change in ownership structure, a change in business model, or a change in trade name in an attempt to hide or avoid the tracking of illicit activity back to its ultimate controller.

DEVELOPED RISK INDICATORS

As part of the analysis within this report, the UAEFIU has developed a list of possible risk indicators that might be directly or indirectly relevant to the abuse of legal persons and arrangements in order to assist reporting entities and stakeholders in identifying the possible involvement of LEs in ML/TF activities. It is pertinent to mention that such indicators can raise suspicion and trigger investigations that lead to further identification of other indicators. Nevertheless, criminal activity cannot explicitly be concluded based on a single indicator. Furthermore, the following indicators should be read together with those previously identified in the UAEFIU report on the abuse of legal entities in 2021 (attached in **Annex 1**).

1. A legal entity has a peculiar, unreasonable, complex structure. It involves multiple ownership layers (especially when offshore or foreign entities are also part of the ownership), combined with difficulties in identifying the UBO(s).
2. A legal entity registered under a misleading name indicates different activities than what the business activity is licensed to practice.
3. A legal entity is registered under a misleading name that appears to imitate other recognized companies' names, particularly high-profile multinational corporations.
4. Potential involvement of a 'shell company,' especially an offshore one, under whose name multiple assets and other entities are being registered, with a suspicion that the primary purpose is to hide the UBO or to disguise fund transfers as a capital transfer for setting up new entities.
5. A legal entity is set up as a front company (the presence of actual business activity; used to commingle legitimate and illegitimate funds, mainly used effectively in cash-intensive businesses).
6. A legal entity's director(s), controlling shareholder(s), and/or beneficial owner(s) or any of its counterparties has been the subject of adverse news from a trusted media source.
7. A legal entity's director(s), controlling shareholder(s), and/or beneficial owner(s) or any of its counterparties who has a nexus to a prominently high-risk jurisdiction that is considered to pose a high risk of money laundering or terrorist financing.
8. A legal entity's director(s), controlling shareholder(s), and/or beneficial owner(s) is listed against the accounts of other legal persons or arrangements, indicating the use of professional nominees.
9. A legal entity or any of its controlling persons or its affiliates is associated with a high-risk or sanctioned jurisdiction, individual or entity.
10. A legal entity frequently or unnecessarily changes shareholders, increases capital, and changes its business name without an obvious rationale.
11. A legal entity heavily engaged in cross-border cash movement, especially if the LE is not registered as a hawala provider, indicates possible illegal hawala activities.

12. Documents provided by a legal entity, such as contracts, invoices, or any trade documents, have vague or missing descriptions, appear to be counterfeit (including false or misleading information), include a resubmission of previously rejected documents, or are frequently modified or amended.
13. Deposits or transfers are received in a legal entity's account, followed by the immediate transfer of similar amounts to another jurisdiction, seemingly a pass-through, leaving a low balance in the account.
14. The circulation of funds between multiple legal entity accounts or between 'unrelated' parties in different lines of business might be suspected of being a 'shell company' (no actual business activity; incorporated for ML purposes exclusively).
15. The number and value of transactions in the legal entity's account do not correspond to the company's activity and transaction history.
16. The transaction structure of a legal entity's account is unnecessarily layered and designed to obscure the true origin of funds, especially high-volume transactions that move rapidly.
17. A legal entity that unnecessarily maintains multiple bank accounts, through which multiple transactions are conducted to circulate the same funds, also involves personal accounts under the name of the LE's shareholders, signatories or UBOs.
18. Several related or unrelated legal entities transfer funds amongst one another, which are referred to as 'borrowing' or 'loan' payments.
19. Establishing/registering multiple entities in a similar or different line of business and activity that are all commonly controlled or registered under the same/repeated shareholder, signatory or UBO(s) name.
20. A legal entity that declares many shareholders and beneficiaries, all of whom are noted to be holding less than 25% of shares, and also many other controlling persons like POAs and authorized signatories.
21. A legal entity account that has demonstrated a long period of inactivity following incorporation, followed by a sudden and unexplained increase in financial activity.
22. A legal entity that fails to declare that any of its directors, controlling shareholders, and/or beneficial owners are politically exposed persons (PEPs) or have familial or professional associations with counterparties that might be linked to PEPs.
23. A legal entity that conducts a large number of transactions (especially wire transfers) with international legal entities supported by trade documents (trade-based) without sufficient corporate or trade justification or when the provided documents are found to be doubtful.
24. A legal entity sends and/or receives frequent payments to/from foreign professional intermediaries without any business justification.
25. A legal entity that receives large funds and subsequently transfers the funds to the personal account of the entity, controlling director(s), shareholder(s), and/or declared beneficial owner(s), or family members.

CASE EXAMPLES

Case example 1: Possible abuse of legal entities through a network of 'shell companies'

The UAEFIU has received multiple STRs/SARs from different reporting entities against **Company A** (a Free Zone entity), which trades in oil and gas. Furthermore, intelligence received from a counterpart FIU implies the involvement of the subject (Company A) in circumventing sanctions.

During the analysis, different counterparties were revealed, such as Company B (same name and owner as those of Company A, but located in a different Free Zone area), Company C, Company D, and Company E. Most of these counterparties (Companies C, D, and E) were found to be operating in different lines of business, such as general trading and goods wholesalers. Moreover, they were subjects of multiple STRs filed with similar concerns.

Company A operates in a high-risk industry (oil and gas trading) without an official business setup or website. The company's transactional activity exhibits a circular pattern within its own accounts as well as other entities in Free Zones (suspected of being shell companies) and offshore companies.

Further investigation has revealed that Company A has had suspicious transactional dealings with high-risk suppliers (Company Y and Company Z) which have had allegations involving sanction breaches and money laundering. Moreover, a public domain search has shown some counterparties having trade nexuses with high-risk jurisdictions.

The analysis suggested that the aforementioned local entities might be acting as shell companies to conceal the ultimate beneficial owner through a circular pattern of transactions and the rapid movement of funds. Consequently, the case was disseminated to the relevant Law Enforcement Agency (LEA) for further investigation.

Risk Indicators:

- Subject is trading in a high-risk industry.
- Subject is dealing with counterparties engaged in different lines of business.
- Subject is dealing with counterparties having previous STR records of similar concerns.
- Subject does not have an official business setup and online presence (website).
- No goods record related to the involved counterparties.
- Company account exceeds its declared annual turnover with the rapid movement of funds.
- Multiple links found with sanctioned individuals or jurisdictions, including the nationality of counterparties' beneficial owner.

Case example 2: The abuse of legal entities in fraudulent activities

Subject A is a new 'sole establishment' owned by a foreign national and established in 2022 for the business activities of 'engraving and ornamentation works, carpentry and wood flooring, and painting contracting.' Subject B is another new 'sole establishment' owned also by a foreign national and licensed on the mainland for the business activity of 'IT infrastructure.' Both establishments were found to be the subject of 7 STRs as well as intelligence (Request for Information 'RFI') from a counterpart FIU for 'fraud' suspicion on the part of different international traders. The owners of said establishments, along with six other similar local legal entities involved as counterparties, misused the accounts of LEs (maintained in UAE financial institutions) to receive funds (suspected foreign fraudulent proceeds) and also were involved in the forgery of signatures, and multiple official documents, to impersonate high governmental officials in the UAE in an attempt to deceive proposed clients (victims) based in foreign countries.

The perpetrator(s) of this scheme alleged to be a representative of a governmental entity that was looking for international vendors of medical supplies such as facemasks and gloves. When a foreign vendor was selected, an amount should have been paid to the (alleged) local entity to register in the local vendor's system, followed by other amounts under different claimed justifications to finalize the trading contract and the deal. Said establishments managed to move over AED24 million from abroad through 36 personal and corporate bank accounts in the UAE.

Ultimately, the FIU issued a freezing order on all involved natural and juridical/legal persons in this scheme and disseminated the case to the concerned law enforcement authority in the UAE.

Risk indicators:

- Newly established legal entity with account(s) activity shows a high volume of transactions that do not match its nature of business.
- Financial institution receives different requests for a 'fund recall' of the customer transaction from correspondent banks.
- Customer fails to provide the relevant documentary evidence to substantiate the transactions in the account.
- Customer statement in the 'Know your Customer' (KYC) is for dealing only in the UAE, while the account shows multiple inward received from entities and individuals abroad.
- Rapid withdrawal of the received funds, leaving the account with major debts.
- Higher turnover than what was declared when the account was opened.
- Counterparty details mentioned in KYC do not match actual transactions in the account.

- Link with a counterparty who has been reported to the UAEFIU due to the same pattern.
- Similar concerns have been received from a counterpart FIU.

Case example 3: The possible abuse of legal arrangements and nominees in the UAE with foreign fraud suspicion

A new customer (**Subject X**) approached a financial institution to establish a family trust in the UAE. The customer was an owner and authorized person of a newly established private company (Ltd.) dealing in a high-risk industry. It was found that Subject X was a family relative of **Subject A**, an ultimate beneficial owner (UBO) who had been subject to adverse media (including World Check) and legal procedures in another country due to fraud suspicion (including buying, selling or managing movable and immovable public funds across the region). According to the UAEFIU database, another SAR was reported by a fund administrator against Subject Y, who was also a family relative of Subject A. Subject Y was a director and beneficial owner of certain entities in an offshore foreign jurisdiction. Based on the foreign country's legal procedures against the customer, financial institutions in the UAE were notified by the UAECB to freeze all subject accounts according to an Abu Dhabi Public Prosecution decision. Ultimately, it was suspected that the customers (Subjects X and Y) were acting as the nominee's shareholding setup, managed by the family of Subject A to run the family business and alleged criminal proceeds.

Risk indicators:

- Use of nominees, trusts, family members, or third-party accounts.
- Holder of the entity's highest shares is the subject or a relative of the subject of adverse media linked to alleged crimes or criminals.
- Entity or beneficial owner deals in high-risk activity or industry.
- Suspicious patterns concerning changes in ownership structure.

Case example 4: The possible abuse of legal entity through point of sales (POS) machines

The UAEFIU received multiple STRs from a reporting entity that facilitates the payment process for merchants using POS machines and online payment systems. The suspicious reports indicated that multiple entities had unusual POS sales volumes. The UAEFIU also received related reports raised by other reporting entities against the involved entities. All involved entities were sole establishments registered on the Mainland.

In most of the involved legal entities, it was found that an individual **(Subject 1)** was a holder of Power of Attorney (POA) for six entities sharing similar licensed business activities (foodstuff

trading, education and training institutes). STRs were raised on four related subjects (counterparties) with the same suspicion: high turnover combined with an unreasonably high amount of POS transactions and remittances, followed by an immediate withdrawal. All transactions involved Subject 1.

Ultimately, it was suspected that Subject 1 was facilitating the layering of funds through the use of front companies, using POS transactions with companies' bank accounts to disguise the origin of the funds. As a result, the UAEFIU disseminated the case to the relevant police department for further investigation.

Risk indicators:

- High value of POS sales for newly established entities with unusual sales which do not make any economic sense.
- Multiple entities controlled by one person holding POA are the subject of different STRs.
- Payment service provider raises multiple reports on the subjects to the UAEFIU.
- Subject entities have declared a common list of suppliers in their KYC, which implies that they are all colluding.

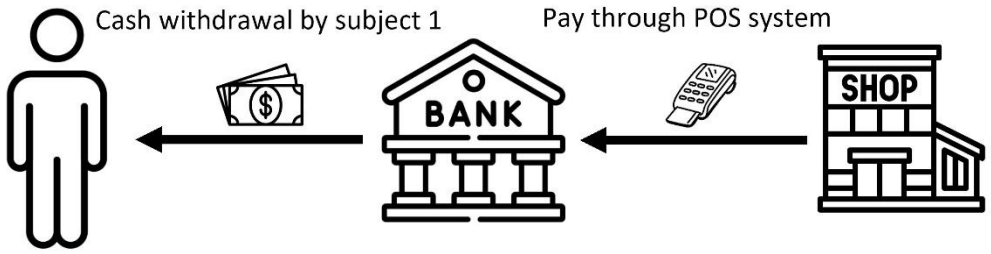


Figure 1 – A simplified illustration on case example 4.

Case example 5: The involvement of DNFBPs in abusing UAE legal entities to move funds across borders

Subject X was convicted in 2015 by a foreign jurisdiction for running fraud schemes involving illegal telephone exchanges by means of a shell company. The UAEFIU investigated the subject based on a suspicious transaction report (STR) from a financial institution in 2021. The STR indicated that Subject X received fraudulent inward payments from six individuals involved in payment diversion fraud in a foreign jurisdiction as well as inward remittances from different entities in different lines of business.

While the subject had no criminal record in the UAE or was the main subject of other reporting entities for suspicious activities, the UAEFIU found that the subject was an owner (with 50% ownership) of a civil company registered on the mainland as a cybersecurity service provider, as well as another limited liability company (with 25% ownership) for car rental services. It was noted that the remaining legal, beneficial owners held the same nationality as that of Subject X. Furthermore, the subject was considerably involved in remittance transactions with a counterparty **(Subject Z)** licensed in one of the UAE Free Zones as a limited liability company for practicing feasibility studies and management consultancies. Subject Z's beneficial owner and POA holder had the same nationality as that of Subject X.

Subject Z was reported to the UAEFIU due to conducting transaction activities that were inconsistent with the declared KYC profile and annual turnover. Subject Z's accounts were mainly funded by international inward remittances from different counterparties in foreign countries. Subsequently, the received funds were routed via online local fund transfers favoring several counterparties in other foreign countries than where the inward remittances were first received. Most of these counterparties had a different line of business, such as recycling metal waste and scrap. These were in addition to local counterparties with a different line of business, such as electronic stores, restaurants, and trading in gold and diamonds.

Ultimately, the subject seemed to be a facilitator of fund movements across different jurisdictions, using UAE financial institutions as well as corporate vehicles of a consultancy assignment to launder the proceeds of foreign predicate offenses (fraudulent) via multilayered international transfers and complex transactions to disguise the ultimate beneficiary owner. This conclusion was due to the rounded nature of the transactions with different counterparties overseas, while Subject X did not provide consultancy project documentation.

As a result, the UAE disseminated the case to the concerned law enforcement agency and sent outward requests for information (ORFIs) to three primary counterpart FIUs. The information received from the counterpart FIUs illustrated that the subject entities located in the UAE were associated with suspicious activity reports filed against said entities' counterparties abroad and that the subjects involved in this case might have been beneficiaries of the reported alleged offenses or involved in money mule activities.

Risk indicators:

- Transactional activity (credit and/or debit) inconsistent with the customer's alleged employment, business, or expected activity, or where transactions lack a business or apparent lawful purpose.
- Actual credit turnover in the account exceeds the declared annual turnover.

- Account funding is mainly from foreign entities and subsequently routed to other foreign entities.
- Supporting documents provided do not justify the account activity.
- Discrepancies in the description of goods or commodities on the invoice or of the actual goods shipped.

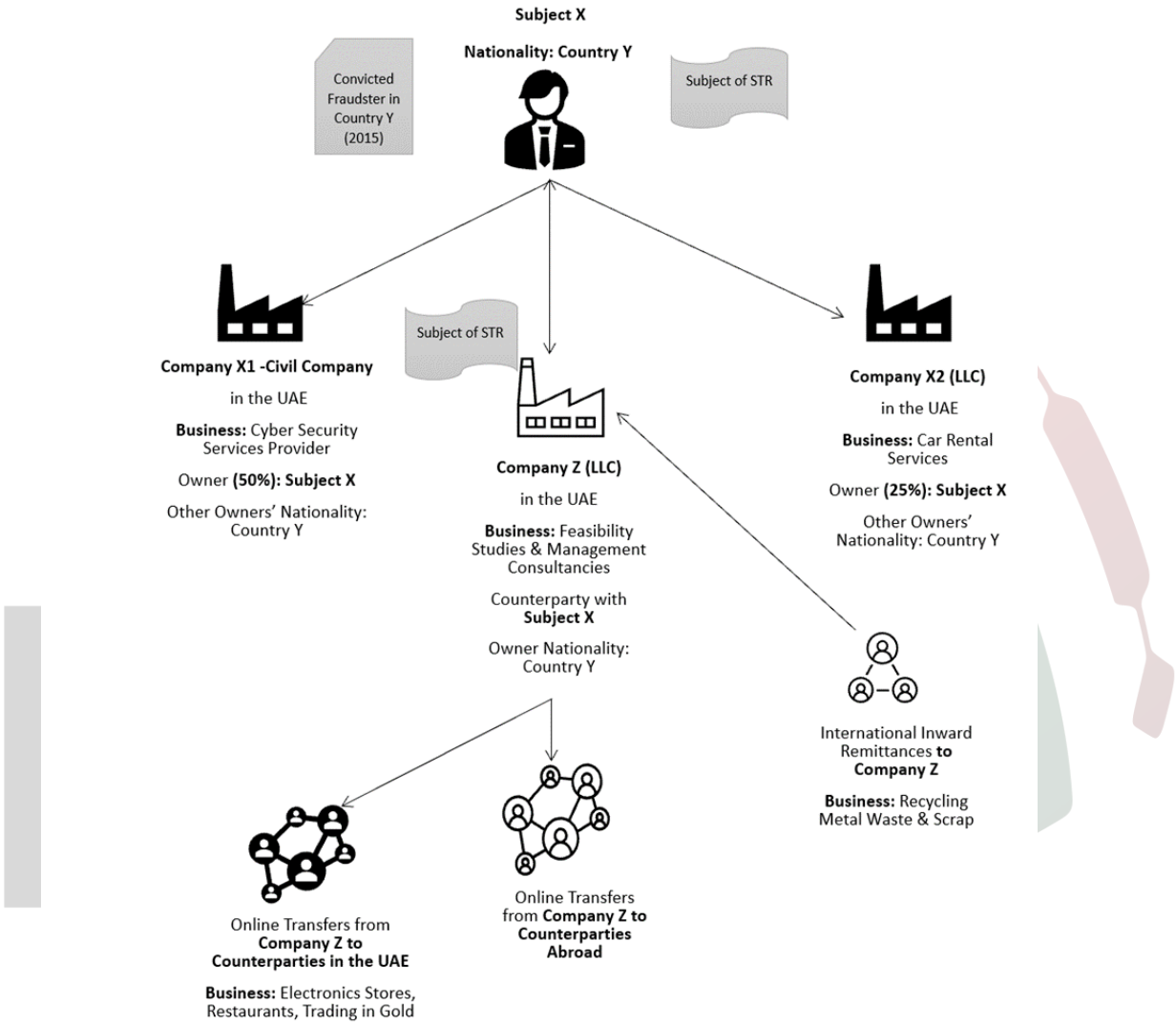


Figure 2 – The involvement of DNFBPs in abusing UAE legal entities to move funds across borders

<u>Case example 6:</u> The abuse of legal entities in possible proliferation financing and sanction circumvention

Company X was a private company established in the UAE for dealing in investment arrangements as an agent or principal. According to the subject's KYC, the company was an execution broker for institutional and individual clients for exchange-traded derivatives, soft commodities, and futures, as well as property and real estate sale brokerage. Company X was owned by Company Z (Ltd.) in the foreign **Jurisdiction A**, which was ultimately owned by three foreign nationals. At the same time, Company X had five different authorized signatories of foreign nationalities, including one of the foreign owners of Company Z. The three foreign owners were subject to a financial penalty imposed by the foreign regulatory authority for their poor management and regulatory standards as well as inadequate risk assessment and governance.

Company X was reported to the UAEFIU for a concern related to potential proliferation financing and sanction circumvention. This was in addition to adverse media regarding the client's counterparties and the large volume and value of transactions, which were inconsistent with the company's anticipated activities (according to its business profile).

The UAEFIU found that Company X was routing high-volume transactions to different counterparties, including local entities licensed for a different line of business and also reported to the UAEFIU for suspicious activities. One of these counterparties was **Company Y**, a local limited liability company licensed to trade in petrochemicals and machinery products. At the same time, it had no business website via searches conducted in open media. It was previously suspected of being involved in shipping the underlying goods with a potential breach of international sanctions. Furthermore, it was suspected of trading in exported goods potentially falling under the Controlled Goods list – Category 10, such as propane and butane. These were in addition to materials such as dimethyl disulfide, perchloroethylene, and methylphenyl acetone. Company Y was found to be dealing with **Company B** (Ltd.) based in the foreign **Jurisdiction B**. According to adverse media, Company B owned and managed shipping companies and vessels. Some of these vessels were suspected of being involved in transferring Iranian crude oil and/or petroleum products.

Furthermore, it was noted that invoices between the local Company Y and the foreign Company B were issued under a similar name to that of Company Y in Jurisdiction B. It was also noted that Company B was registered in different jurisdictions and associated with counterparties reported in the Panama Papers.

Another counterparty of Company X was **Company Z**, a limited liability wholesaler registered on the UAE mainland. Company Z was also suspected of a potential breach of international sanctions while conducting business with two counterparties (LLC) based in the UAE and other jurisdictions, including Iran. As such, these UAE companies were suspected of acting as front companies on

behalf of Iranian-based entities or individuals. For example, one of these local entities had a similar name to an entity that was the subject of the US OFAC SDN list.

Ultimately, while it was challenging to establish a solid ground for Company X's involvement in PF activities, and there were no further details shared on the end user and the country of destination of the company's shipments, the company appeared to be a front or intermediary. The suspected purpose of the company's activities was to conceal the final destination of goods/transactions of the beneficial owner through customers' engagement in complex, suspicious arrangements. Therefore, the case was disseminated to state security.

Risk indicators:

- Customer or transaction is suspiciously involved in the supply, sale, delivery, export or purchase of dual use.
- Customer is suspected of working for, acting on behalf of or controlled by a sanctioned individual, group or entity.
- Transactions are inconsistent with the account's normal activity.
- Inconsistent transactions or remittances with the customer profile received from third parties.
- Account shows a high velocity in the movement of funds.
- Suspicion of unregistered hawala activities.
- Lack of appropriate documentation to support transactions.
- Adverse media reports or negative news that the account holder is linked to alleged crimes or related to criminals.

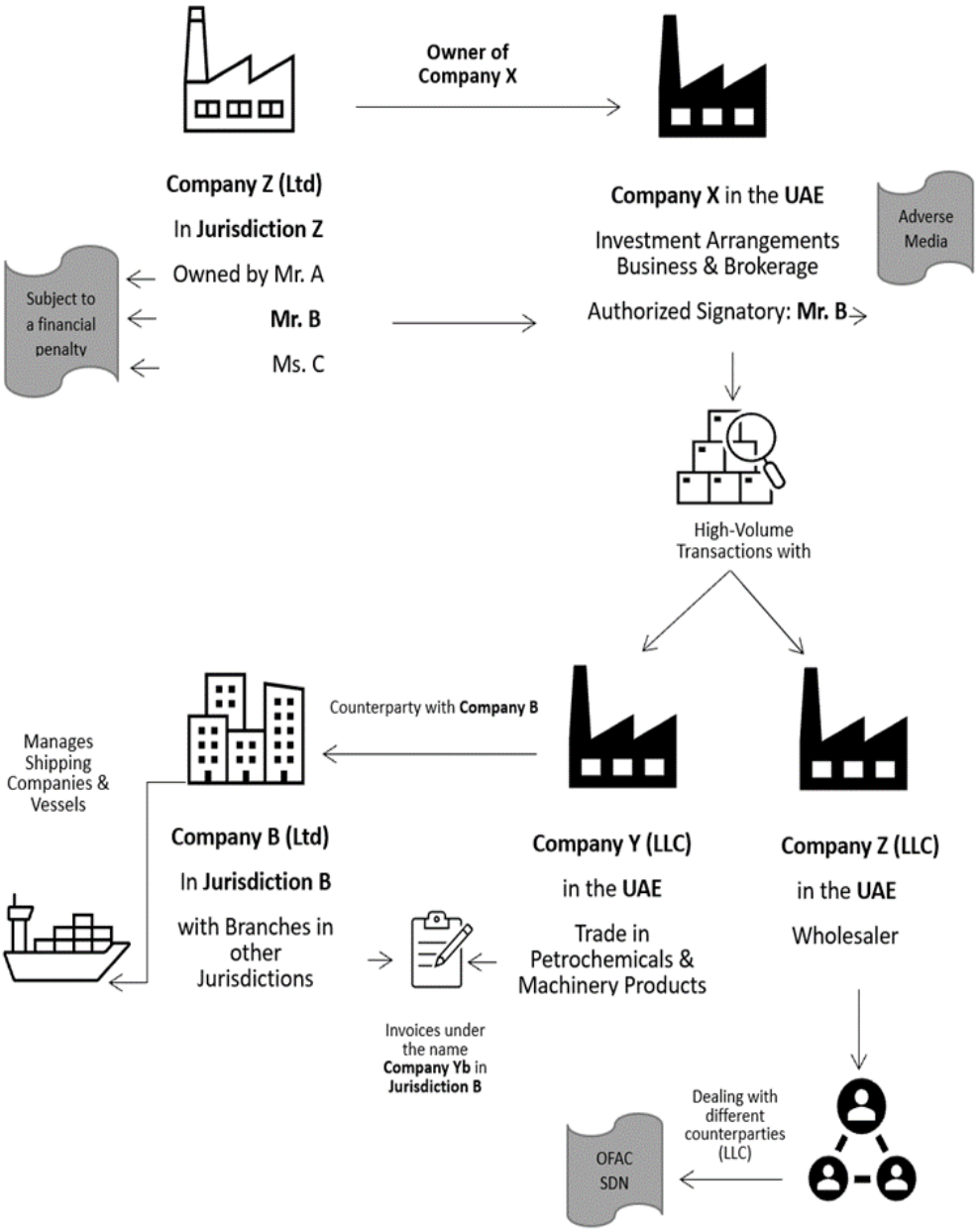


Figure 3 – The abuse of legal entities in possible proliferation financing and sanction circumvention

CONCLUSION

This report identified different patterns related to the abuse of legal persons in illegal activities. It developed a list of risk indicators to be considered together with the one previously identified in 2021. Reporting entities and registrars should update their risk indicators and monitoring systems accordingly.

This report underlined that legal entities willingly or unwillingly are misused in mingling illicit funds with legitimate businesses or in moving funds from one jurisdiction to another, all in an attempt to deprive the illicit funds of their origin as well as actual ownership in order to harden the ability of LEAs to trace them. The easy passage of funds and the variety of financial and trade transactions available are ideal vehicles for the layering stage of money laundering.

Furthermore, this report suggested that the misuse of legal entities involves not only the financial system but also the trading system and DNFBPs, whether in money laundering layering and integration stages, sanction circumvention, or proliferation financing. At the same time, some observations were noted concerning the possible involvement of legal entities in drug trafficking. However, such observations will be thoroughly considered in the following strategic analysis report on 'Narcotic Drugs Trafficking, Trends and Typologies' planned in Q3 2023.

For reporting entities, it was noted that some STRs/SARs did not clearly indicate the suspicion and the reason for reporting, while only submitting a list of transactions. In other incidents, some reporting entities did not include any clarification in the reporting system textbox or submitted their own conducted STR/SAR. Moreover, transaction amounts and counts uploaded into the system did not match the transactions contained in the suspicious report. What is more, few suspicious activities and transactions were reported under other types of reports. Reporting entities are encouraged to enhance the quality of their reported suspicious activities and transactions. This should include a clear reference as to whether the subject is an entity or individual as well as the reason for the reporting and suspicion.

Lastly, it was also noted that some reporting entities considered the registered legal shareholder to be the ultimate beneficial owner. As such, reporting entities should ensure, through their training programs, compliance officers' awareness of the difference between a legal shareholder and an ultimate beneficial owner. In all situations, reporting entities should indicate the process undertaken in tracing an ultimate beneficial owner as well as the reasons or challenges encountered in identifying the ultimate beneficial owner and when a complex structure is noted.

ANNEX 1 – Risk Indicators developed in previous report on the Abuse of Legal Entities in ML/TF (first report in 2021)

1. Transactions that appear more complicated by use of impressive but nonsensical terms.

2. Circulation of funds between linked or related entities accounts using different type of instruments (cheques, electronic transfers, etc.).

3. Large volume of cash transactions through different branches of the financial institution, specially conducted by multiple individuals.

4. Transactions structure appears unnecessarily layered and designed to obscure the true origin of funds.

5. Multiple parties collaborating in a single transaction.

6. Multiple entities remitting a single or repeated beneficiary (also entity) of which the funds subsequently remitted to offshore entity.

7. 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.

8. A legal entity does not have adequate presence or the mere presence conveys ambiguity, i.e. online presence through websites that are vague.

9. A legal entity has a beneficial owner/ultimate beneficial owner or associates with known dealings with counterparties residing in high risk or sanctioned jurisdictions.

10. A legal entity or its beneficial owner/ultimate beneficial owner is linked to a negative/adverse media reports.

11. 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.

12. 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.

13. A legal entity is newly established and observed to have engaged imminently to high volume of transactions and business activities.