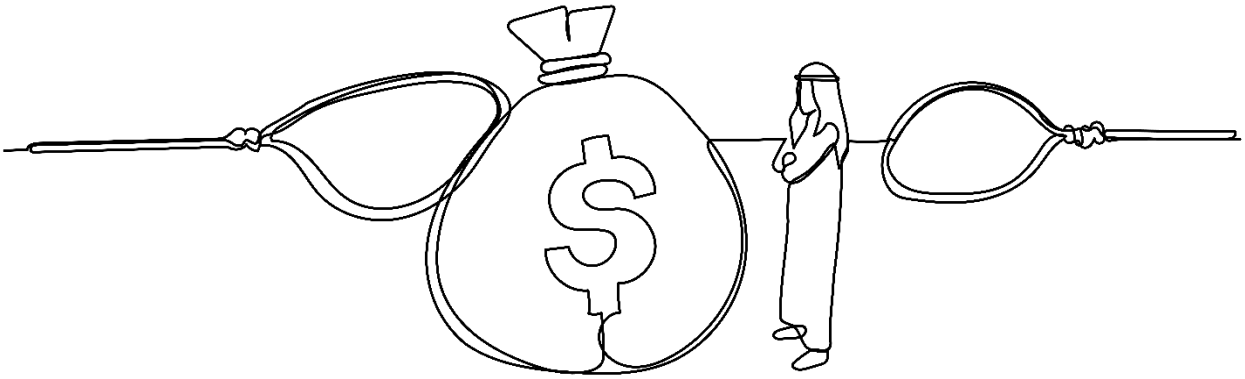
وحدة المعلومات المالية
Financial Intelligence Unit

Financial Crime Typologies in the Financial Sector

Summary Report

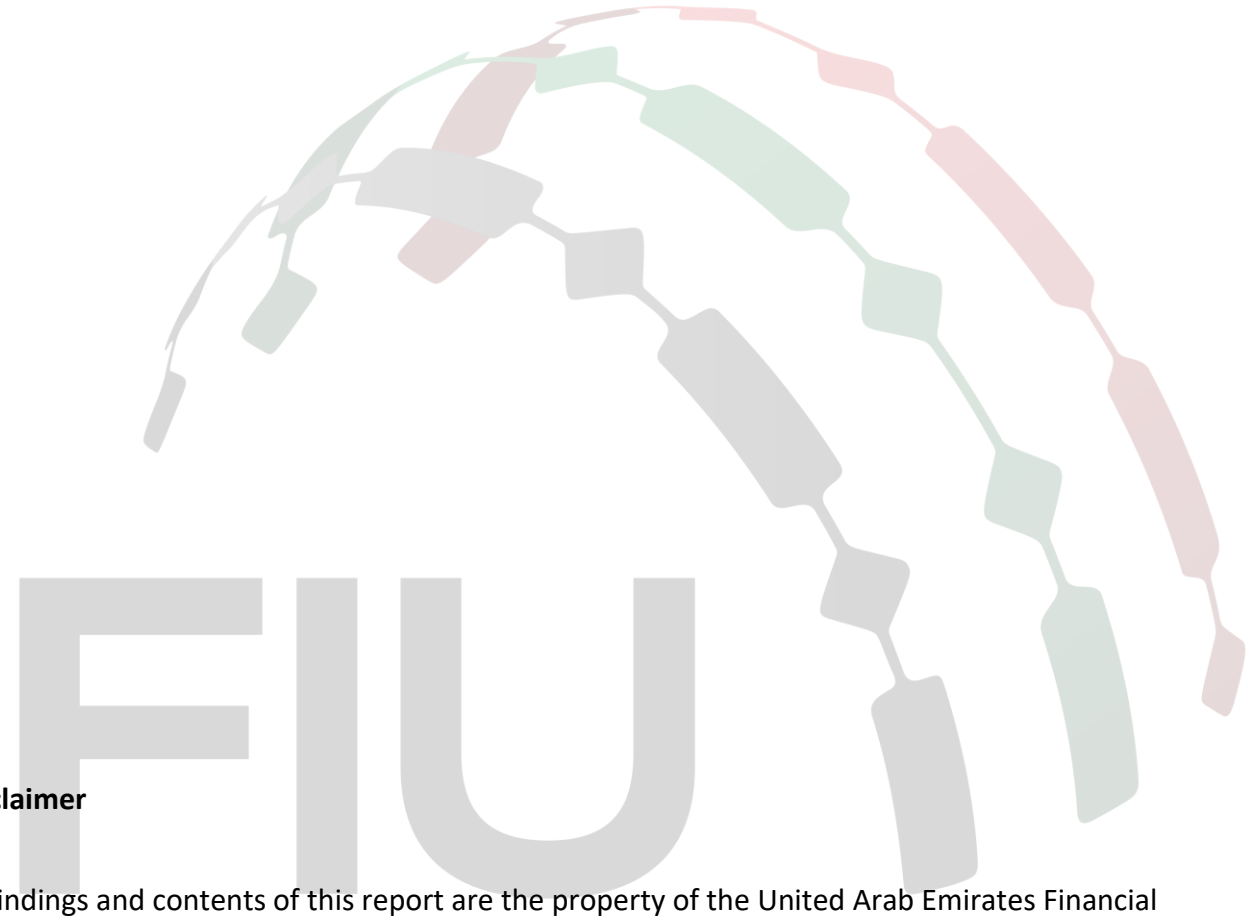
January 2024



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

DNFBPs	**Designated Non-Financial Businesses or Professions**
DPMS	Dealers in Precious Metals and Stones
FATF	Financial Action Task Force
FIs	Financial Institutions
goAML	The Financial Intelligence Unit Reporting System
LoC	Letter of Credit
LP	Legal Person
ML	Money Laundering
MSBs	Money Service Businesses (MSBs)
NRA	National Risk Assessment
PEP	Politically Exposed Person
PML	Professional Money Laundering
PMS	Precious Metals and Stones
RHPs	Registered Hawala Providers
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
TF	Terrorist Financing
CSP	Company Service Provider
UAEFIU	UAE Financial Intelligence Unit
UBO	Ultimate Beneficial Owner
UHP	Unlicensed Hawala Provider

Introduction

Criminals often exploit the financial sector to move their ill-gotten gains of crime and conceal their origin due to financial institutions' (FIs) extensive cross-border networks and their accessibility to a variety of products and services. Criminals may resort to employing other channels and techniques such as establishing front or shell legal entities, using trade-based money laundering, or cash smuggling, among others. Still, the ultimate purpose would be to open accounts with financial institutions to move their money swiftly across borders.

As identified in the UAE's first National Risk Assessment (NRA) and noted by the Financial Action Task Force (FATF)'s mutual evaluation in 2020, the UAE is exposed to money laundering (ML) and terrorist financing (TF) risks due to certain inherent risks. These risks are associated with the expansion of the financial and commercial free zones, the large size and openness of the UAE's financial sector, and the large amount of remittances.[1]

In order to mitigate the ML/TF risks in the financial sector, the FATF Recommendations allow countries' competent authorities to assess and decide on the most appropriate and effective way in which to mitigate the ML/TF risks associated with the financial sector. By following a risk-based approach, supervisory authorities, as well as financial institutions, would be able to establish an assessment of high and low ML/TF risks involved in the sector and decide on the extent and severity of the required AML/CFT controlling measures, e.g., whether simplified or enhanced measures are required in order to mitigate the identified risks.

As per FATF guidance on applying a risk-based approach to the financial sector and assessing the sectoral risks, it is advised to "include, but will not be limited to, the jurisdiction's national risk assessments, domestic or international typologies and supervisory expertise, as well as Financial Intelligence Unit (FIU) feedback."[2] Accordingly, this report aims to share the UAEFIU's relevant findings on **money laundering typologies in the financial sector.**

This report addresses the financial crime typologies categorized by frequently observed predicate offences that are contributing to money laundering, alternative banking services and underground banking, and trade system and trade-based money laundering techniques. Moreover, the Basel AML index shed light on DNFBPs' ML/TF risks: "Lawyers, accountants, real estate agents, casinos, precious metal dealers, and other so-called designated non-financial businesses and professions (DNFBPs) are significantly less protected against ML/TF risks than financial institutions."[3] Therefore, this report also underlines high-risk sectors of designated non-financial businesses and professions (DNFBPs) and their links to the financial sector.

Target Audience

Financial institutions regulated by the Central Bank of the UAE (CBUAE), the ADGM-Financial Services

[1] FATF (2020) 'Anti-money laundering and counter-terrorist financing measures: UAE mutual evaluation report'.

[2] FATF (2014) 'Guidance For A Risk-Based Approach: The Banking Sector', p. 13.

[3] Basel AML Index (2021) 'Money laundering risks: are we paying enough attention to lawyers, accountants and others beyond the financial sector?'.

Regulatory Authority (FSRA), and the DIFC-Dubai Financial Services Authority (DFSA), are the main target audience of this report. The outcome of this report has been shared previously by the UAEFIU with reporting entities from financial institutions based on topics introduced in the UAEFIU-published typology reports. This synopsis summarizes identified typologies directly relevant to the financial sector, highlighting major risk indicators.

Methodology

This report illustrates major typologies and patterns of abusing the financial sector in the UAE through different financial crimes over the span of four years. This brief report is a collective work consisting of the UAEFIU typology reports published **during 2021–2023** on different topics. Further information and comprehensive analysis are available in the UAEFIU-published typology reports.

The outcome discussed in this report is based on an analysis of different samples of data available within the UAEFIU's databases, particularly Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) reported to the reporting system (goAML), cases disseminated to law enforcement authorities (LEAs), as well as cases and freeze requests available in the Integrated Enquiry Management System (IEMS). These are in addition to reports related to international requests (Inward Spontaneous Disseminations, Inward Requests for Information, Outward Spontaneous Dissemination, and Outward Requests for Information). The UAEFIU databases were used along with other data and insights received from the concerned supervisory and regulatory authorities.

While each topic had its own methodology, all typology reports involved the examination of a sample of the aforementioned data covering one previous year (as a minimum) or three previous years (as a maximum), depending on the topic methodology. The total examined samples during the aforementioned timeframe included **6729 suspicious reports received from different reporting entities and over 500 international requests.**

Findings

A. Predicate Offence and Money Laundering Typologies

1. Drug Trafficking and Money Mules

According to the FATF 4th round of Mutual Evaluations, two thirds of countries have identified drug trafficking as a major predicate offence involving money laundering, followed by corruption, fraud, and tax crimes.[4] Organized crime groups (OCGs) generate billions of dollars annually from their trade in illicit drugs. Therefore, OCGs use a wide range of methods to launder their proceeds, such as cash smuggling, abusing financial institutions' services, establishing shell companies, and employing trade-based money laundering techniques and the services of professional money launderers.[5] **The typical patterns employed in drug trafficking and money laundering in the UAE include, but are not limited to, the following:**

- *Money Mules*

The typical pattern identified is observed when a blue-collar[6] or low- to medium-income worker[7] opens a saving account to receive a salary but uses it as a funnel account for drug trafficking. The account usually shows multiple cash deposits through the use of ATMs/CDMs in different locations across the UAE in a very short span of time by multiple individuals, which appear to be made by third parties and subjects of different nationalities. Amount values range from AED100 to AED5000, but high amounts have also been observed (ranging from AED9000 to AED30,000).

Subsequently, funds are directly withdrawn from the account through ATM cash withdrawals, internal account transfers, and/or outward transfers to one's own account or the accounts of other individuals/entities maintained with either the same financial institution or another local financial institution in the UAE.

Therefore, the account's activity in this typical pattern often shows a noticeable and sudden surge in deposit and withdrawal activities over a short period. Additionally, the analysis revealed that following the closure of many subjects' bank accounts, due to the bank's concern regarding the customer's unusual transactions, the subject would open a new account with another bank or use one of their dormant accounts.

The same mule could also abuse money service businesses (MSBs) to receive or transfer multiple funds related to drug trafficking. The alleged drug trafficking funds would be collected from the mules and transferred through the MSBs via multiple structured amounts to specific beneficiaries abroad. In cases involving foreign jurisdictions, the beneficiary in the foreign country could be a natural or legal person (LP). Exchanging different amounts of currencies is also common in this pattern, with mules perhaps also approaching the MSBs in a group of individuals who will split an amount between them to avoid the detection and reporting threshold.

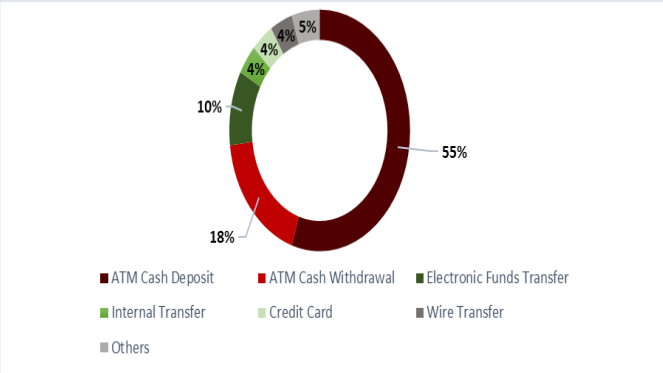
[4] FATF (2022) 'Report on the State of Effectiveness and Compliance with the FATF Standards'.

[5] FATF (2022) 'Money Laundering from Fentanyl and Synthetic Opioids'.

[6] Blue-collar worker refers to individuals who usually engage in hard manual labor, typically in agriculture, manufacturing, construction, mining, or maintenance sectors, and truck drivers.

[7] Still, this pattern is also observed in account owners held managerial positions in different companies or partners.

CHART 1–*Main mode of transactions employed*



- *Abusing Legal Person Accounts in Drug Trafficking*

The most common pattern in abusing legal structures in drug trafficking is through establishing a network of legal persons, such as cleaning service companies, electronic shops, or cash-intensive businesses. A legal person would receive cash deposits from multiple individuals and other companies (counterparties) with different business lines, followed by immediate cash withdrawals and outward clearing cheques. The legal person's bank account would be combined with the mules' accounts to funnel and layer the deposited cash.

The majority of entities involved in the sample examined (93 suspicious reports), were established on the 'Mainland' with an approximate percentage of 65%, and 30% were established in the 'Free zone', while the remaining 5% were identified as 'unknown' as their information was not provided by the reporting entity. With respect to entities' legal forms, they were mainly licensed as 'Limited Liability Company', followed by 'Sole Establishment'.

- *Laundering the Proceeds of Drug Trafficking*

To possibly launder the proceeds of drug trafficking, the observed pattern is that of an account witnessing two transactional patterns: the first relates to the typical pattern identified previously (cash in and cash out), while the second underlines multiple highly structured amounts and the layering of cash from unknown sources. In such a case, the account owner might merely be a mule or one of the masterminds behind laundering the proceeds of illicit activities associated with organized crime.

Another pattern revealed unjustifiable immediate debits to third parties or independent accounts of individuals or entities after accumulating small cash deposits. Transferring and moving such funds or changing their form suggested typical characteristics of money laundering.

In most reported suspicions of laundering the proceeds of drugs, screening results and adverse media were the major factors that enabled reporting entities to link their customers' unusual transactions to the suspicion of drug trafficking proceeds.

- *Major Risk Indicators* [8]

- Account activity shows high velocity in the movement of funds.
- An account is suspected of being used by a third party, especially if the account holder appears to be non-resident or outside of the country.
- An account that is only funded via inward remittances and cash deposits.
- An individual opens an account whose purpose is a salary transfer with no actual salary credits found in the account.

[8] For further risk indicators, please review the UAEFIU report 'Patterns of Abusing Financial Institutions in Drug Trafficking and Laundering its Proceeds' issued in August 2023.

- An individual opens multiple accounts with different financial institutions without a reasonable purpose or that are inconsistent with the customer profile and income.
- An individual account opened for salary or savings purposes shows multiple cash deposits inconsistent with the customer profile, followed by immediate structured withdrawals from different locations on the same day Or consecutive days.
- An individual or a group of individuals conducts multiple foreign currency exchange transactions with a money service business that involve multiple currencies.
- An individual or a group of individuals approaches a money service business to conduct multiple transfers to a single or frequent beneficiary, especially if the beneficiary is located in a jurisdiction known for drug trafficking.
- A company that trades in drug substances receives payments from a foreign legal person(s) based in a jurisdiction known for drug trafficking.
- A company account shows frequent cash deposits in relatively small amounts, followed by multiple transfers to different individuals and legal persons where the relationship between the parties and the purpose of the transactions are not established.

2. Fraud

Fraud instances have been witnessing a dramatic increase globally, especially since 2019 and more incidents are expected to occur in 2024.[9] According to the UAE NRA, fraud is one of the major predicate offences leading to money laundering, and received a rating of high risk accordingly.

In terms of fraud transaction modes, funds transfer fraud (or money transfer fraud) was observed to be the most typical transaction mode used in fraud and usually involves a significant amount of funds. Funds transfer fraud in most cases is followed by a **'funds recall request**' sent by the remitting bank (victim's account) to the beneficiary bank (account of perpetrator or fraud accomplice).

The fraudulent funds received in the perpetrator's account are usually dissipated rapidly by either cash/cheque withdrawals or being subsequently transferred to another account(s), as in more complex cases.

Moreover, using shell entities in fraud transactions was considerably observed in many scenarios, especially when the original fraudulent activity occurs in a foreign country, with the proceeds being routed to the UAE, particularly to accounts held by legal entities.

Said accounts either are controlled by the fraudsters directly or their allies or are controlled by gatekeepers in more sophisticated fraud operations (such as company service providers). 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.

[9] Unit21 (2023) 'State of Fraud and AML', Vol. 02.

Overall, **the following are the most common fraud types observed by the UAEFIU:**

- *Impersonation fraud and Business Email Compromise (BEC)*

This is one of the main concerns that counterpart FIUs have mostly queried. It refers to a type of cyber-attack (usually via hacking or phishing) and would involve impersonating a company's official to conduct unauthorized transactions.

This scheme generally starts with either the exploitation of publicly available information or the hacking of an individual's or organization's email (spoofing). After obtaining sufficient information that could be used for the commission of BEC fraud, perpetrators typically use other prevalent techniques to deceive victims.

- *Scam Fraud*

There are different types of fraud scams observed, with the commonly used techniques in this fraud type as follows:

- **Advertising for fake products** via social media platforms and bogus sites. The most popular pattern consists of employing 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 a natural or legal person account, the buyer receives no actual goods.
- **Fake Visa/Ticketing fraud** in which perpetrators act as a legal travel agent offering a visa or ticketing service and asking for the payment to be completed online before proceeding to the issuance of the visa or ticket. After the transfer has been made, the travel agent poseur stops communicating with their victim.
- **Investment scam**, which is one of the most popular fraud types in which the perpetrator tends to offer an investment (more often fictitious) to their target with the promise of a high return with little or no risk. Prospective investments in this type of fraud are usually in three forms: company shares, real estate, and stocks. Investment scams could also use other fraud schemes against the same victim, e.g., **romance fraud**, by luring victims of romance digital platforms into claimed investment schemes.

  One commonly observed transactional pattern in **'investment fraud'** is that of using legal persons to receive funds from prospective investors and then routing the funds through multiple LP accounts.

  The entity usually 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 LP accounts, allegedly toward business-related entities/counterparties. Some entities might use misleading and deceptive names similar to those of trusted, popular establishments in the UAE to gain the victim's trust and defraud them.
- **Online scam through virtual currencies**, which involves entities promoting crypto-investments and misleading victims to invest in digital currency products that they have offered, which have had on some occasions no monetary value. As such, the victims are lured toward the fake promise of obtaining high investment returns after virtual assets/currencies are transferred to the fraudster's wallet address. Subsequently, the fraudster either

stops communicating with the victim or continues to extort more virtual assets by asking the victim to send more as a "fee" in order for the principal amount to be returned along with the supposedly promised "return." The UAEFIU has also received different intelligence reports from counterpart FIUs regarding similar concerns (e.g., virtual currency Ponzi schemes).

- *Phishing/Vishing*

Fraudsters obtain the victim's sensitive information or credentials either online (phishing) or via phone calls (vishing). In phishing attacks, the victim would usually need to click on a malicious link that would ask them to enter their information on the background. This 'click' might download malware or viruses to the device used by the victim, enabling the attacker to obtain all entered information. In the most common scenarios, the attacker will create a fake or what looks like the website of a financial institution and will give the victim some steps to follow. In vishing, meanwhile, fraudsters use different ways and social engineering techniques to convince victims to reveal their personal or sensitive information willingly over the phone.

- *Forgery and Counterfeit*

Forgery usually involves altering an instrument or document with the intention to deceive another party, such as **'signature forgery**' or **'cheque forgery**,' which involves making unlawful alterations to details such as the amount, or it might be paired with signature forgery. Counterfeit, on the other hand, involves making an imitation of a genuine instrument or document, such as creating totally false identity documents, making fake cheques or counterfeit currencies, and generating false invoices.

- *Major Risk Indicators* [10]

- A customer submits documents suspected to contain any materially false, fictitious or fraudulent statement or entry.
- Discrepancies are observed between reported facts, observed data, and/or supporting documentation.
- Inadequate or apparently altered supporting documentation (such as alterations to any vital information, scraps, spelling mistakes, etc.).
- An incoming funds transfer followed by a 'funds recall request' from the remitting bank.
- Funds recall requests are received from different remitting banks on the same beneficiary.
- Funds are received via wire transfers (international or local) from unrelated parties, followed by immediate withdrawals or outward remittances.
- Frequent incoming funds transfers from unrelated parties to a newly opened account(s).
- Unusual transactions or inter-account transfers (including relatively small amounts).

3. Corruption and Politically Exposed Persons (PEPs)

[10] For further risk indicators, please review the UAEFIU report 'Fraud Crimes, Trends & Typologies' issued in 2021.

The international standard requirements concerning corrupted politically exposed persons (PEPs)[11] are measures that are preventative (not criminal) in nature. Still, PEPs are often subjects of international requests received from FIU counterparts, including their family members and associates. Similarly, in many subject cases of STRs/SARs reported to the UAEFIU, PEPs were found to be using their family members or third parties to receive funds from different jurisdictions.

The PEP might be indirectly linked to a complex structure of foreign and local legal persons. Corrupted PEPs also have a higher tendency toward using professional money launderers. Overall, different suspicious reports uncovered accounts of PEPs in the form of high-ranking public officials or company executives who were linked to perpetrated fraud, embezzlement, corruption or bribery in their home countries and who siphoned off illegally obtained funds to the UAE.

- *Major Risk Indicators*
- A customer falls under the definition of PEPs as indicated in Cabinet Decision No. (10) of 2019 and is from a country with a high level of corruption.
- A customer has authority, regulatory approvals, access to funds and assets, and control over a public fund.
- An unexplained source of wealth with no supporting documents.
- Funds are repeatedly moved to and from countries with which the PEP does not seem to have ties.
- The customer intentionally provides false, misleading or incomplete information.
- The use of third parties (including family members or close associates and intermediaries) in conducting business and transactions.
- The use of corporate vehicles to conceal the identity of a beneficial owner or source of funds.
- Relationships between parties (natural and legal persons) involved in the customer transactions are obscured.

4. Tax Evasion and Laundering its Proceeds

Different suspicious reports implied that legal persons are being misused in the UAE for possible tax evasion purposes, particularly, entities established in free zone jurisdictions and licensed to provide consultancy and advisory services. Usually, adverse media related to tax evasion cases in another jurisdiction trigger suspicious reporting on a legal entity for possible laundering of the proceeds of tax evasion.

One of the common patterns consists of a legal person importing or exporting goods through under-invoicing to intentionally manipulate the price of goods (as opposed to their market value) so as to pay lower tax duties. This pattern could also be combined with routing funds through shell companies to disrupt the money trail.

Another pattern involves various predicate offences 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**'

[11] As per Article (1) of the Cabinet Decision No.(10) of 2019, Politically Exposed Persons (PEPs) are "Natural persons who are or have been entrusted with prominent public functions in the State or any other foreign country such as Heads of States or Governments, senior politicians, senior government officials, judicial or military officials, senior executive managers of state-owned corporations, and senior officials of political parties and persons who are, or have previously been, entrusted with the management of an international organisation or any prominent function within such an organisation".

or '**missing trader fraud**',[12] which is essentially a type of VAT fraud that attempts to exploit a jurisdiction's VAT rules through an indirect series of repeated trade-based transactions and activities.

Data analysis also illustrated possible laundering of proceeds related to tax evasion through buying real estate in the UAE, e.g., through a broker or tax advisor holding POA to act on behalf of foreign offshore and limited (LTD) companies in selling and purchasing properties in the UAE.

- *Major Risk Indicators*[13]

- The use of several bank accounts receiving large deposits from different sources.
- A legal person that does not conduct real operations (Shell Company).
- Using false information and documents (including false and stolen identities to set up businesses).
- Large unusual claims and deductions, or similar claims all made in the same manner or format.
- Using tax refund or rebate by filing of false information.[14]
- Transactions involving tax havens.
- Under-invoicing in the real estate sector.

B. Alternative Banking System and Underground Banking

1. Money Service Businesses (MSBs) and Registered Hawala Providers (RHPs)

The UAE NRA concluded that money service businesses (MSBs) and registered hawala providers (RHPs) are involved in medium–high-risk crimes such as terrorist financing, fraud and professional money laundering. Similarly, the UAEFIU observed the same pattern of fraudsters abusing MSBs to receive fraudulent funds from victimized individuals. In addition to said observation, **the following are the most commonly identified typologies involving MSBs in illicit activities:**

- *Cash Border Movements*

Cash border movements often involve individuals carrying cash from diverse nationalities arriving from various jurisdictions to the UAE. Cash transported is in different currencies and is declared to the local customs authority in favor of a legal person or exchange house. The findings suggested that there could be a couple of possible scenarios regarding this: (1) Funds' beneficiary is only a front/shell company whose role is to receive funds on behalf of an MSB; (2) Funds are directly declared for an MSB which is possibly conniving with a third party to launder the proceeds of crime.

- *Layering of Funds through the Exchange of Foreign Currencies*

A common method of '**layering**' is that of exchanging monetary instruments, converting cash

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

[13] OECD (2006) 'Report on Identity Fraud: Tax Evasion and Money Laundering Vulnerabilities'.

[14] A tax refund, as the name suggests, is when a taxpayer pays more than his/her liability so that the government would return the excess amount. However, a tax rebate entails various exemptions and deductions on taxable income to be reduced by means of tax rebates.

into other currencies to mislead financial investigators of its actual source and purpose. In such a pattern, documents or invoices used to support the source of a currency in hands (e.g., Declaration Regarding Importation of Cash (DRIC)) could be forged or altered.

- *Major Risk Indicators* [15]

- A customer remits money internationally and then receives in return an equal value of the amount.
- A customer presents a single DRIC as supporting documentation for multiple transactions.
- A customer receives multiple transfers from unrelated parties, specifically individuals residing in a foreign jurisdiction, on which a "fund recall request" has been received.
- Using the account of an MSB or RHP to send or receive funds which are suspected to be fraudulent proceeds.
- A customer (sender) appears to have no direct or economical relationship with the receiver of the transfer.
- An individual account is receiving small amounts from different unrelated individuals, eventually transferring the sum to another natural or legal person's account.
- A group of customers use similar contact information with an unreasonable explanation (e.g., address, mobile number, email address).
- A customer is suspected of acting on behalf of a third party but not disclosing that information or is being controlled by someone else.
- Transactions conducted in the account are unnecessarily complex with no apparent economic rationale.
- Several transfers from multiple remitters are directed toward a single beneficiary with no reasonable explanation.

2. Unlicensed Hawala Provider (UHP)

An unlicensed hawala is a common concern amongst other FIU counterparts. In different cases, the analysis indicated that legal persons were suspected of engaging in unlicensed/unregistered hawala (UHP) activities with the absence of a 'Hawala Provider Certificate' granted by the CBUAE in addition to their primary commercial/business activities being licensed by other licensing authorities. UHPs tend to commingle funds specific to hawala activities with the usual funds resulting from regular business activities (as front companies). Another technique is to use shell entities for the purpose of conducting unlicensed or illegal hawala activities.

It is also assumed that the commonly used technique of settlement is the **'reverse hawala'** between two or more hawala providers within the same network, during which they exploit trade transactions (TBML techniques), with settlements conducted through wire transfers, or using cash couriers and cross-border cash movements for cash settlements.

The entities involved in UHPs were mainly in the business of 'general trading,' 'foodstuff,' or 'dealers in precious metals and stones,' and the majority

[15] For further risk indicators, please review the UAEFIU report 'Money or Value Transfer Services (MVTS) and Registered Hawala Providers (RHP)"'issued in 2021.

were found to be established as LLCs and incorporated in mainland jurisdictions.

The acting unlicensed hawala was also observed in third party accounts receiving a high volume of credit transactions from multiple ATM cash deposits and inward remittances from different individuals and entities — i.e., general trading companies. The credit amount might also involve receiving a high value of clearing cheques. Different STRs also suggested possible involvement of hawala service providers in changing cryptocurrency to manager cheques or cash.

- *Major Risk Indicators*[16]
- A legal person (suspected UHP) conducts an unusually high number of transactions with counterparties (known HPs) in high-risk jurisdictions or provides services to customers from high-risk jurisdictions.
- A legal person (suspected UHP) structures transactions in an attempt to break up amounts to avoid reporting or interrupt the tracing of funds.
- A legal person's transaction volume is inconsistent with its stated business activity, scope, or past transaction volume.
- A legal person (suspected UHP) is heavily engaged in cash border transactions involving high-risk jurisdictions.
- A legal person's (suspected UHP's) owners, shareholders, or authorized signatories, or any of its counterparties, have been the subject of adverse news from a trusted media source.

A legal person (suspected UHP) seems to use trade transactions to settle accounts between jurisdictions, precisely TBML techniques like over-invoicing or under-invoicing.

3. Far Eastern Underground Banking

Far Eastern underground banking is recognized by financial institutions (FIs) in the UAE since 2017. UAE FIs were detecting legal entity clients receiving unreasonably high volumes of large cash transaction activities followed by multiple outward remittances to/through Far Eastern countries. Thereafter, the scheme continued to employ rapid movements of funds but through more intersections of different transaction modes, including inward wires from multiple counterparties, internal transfers, cash and cheque deposits, clearing cheques, or through customers' own accounts. Subsequently, these transactions are wired outward to customers' own accounts or to other entities' accounts in the country and abroad. Most outward transactions headed to multiple destinations in Far Eastern countries.

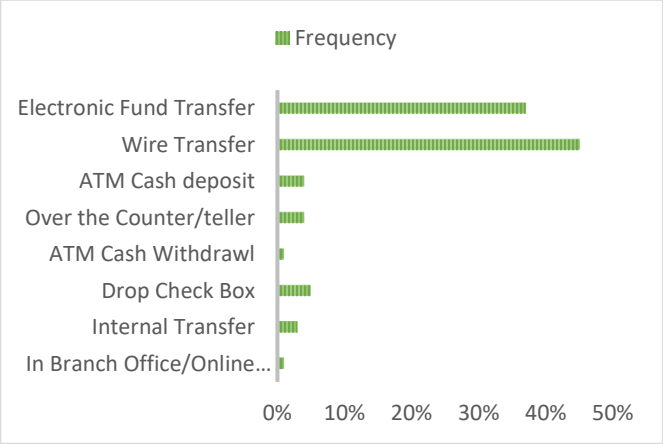
The most common techniques used in this typology are the following:

- Frequent electronic transfers and deposits of a large amount of cash or cheque deposits followed by an immediate withdrawal/ transfer to common Far Eastern countries.
- A high volume of transactions are conducted by multiple legal entities owned or managed by the same nationality.

[16] For further risk indicators, please review the UAEFIU report 'Money or Value Transfer Services (MVTS) and Registered Hawala Providers (RHP)' issued in 2021.

- The amount of entity turnover and inward transactions is inconsistent with the nature of business income.
- An unexplained source of income or purpose of account activities.
- Possible document and trade invoice fabrication and price manipulation.
- Potential utilization of unlicensed hawala.

CHART 2–*Most Frequent Transaction mode involved in Far East Typology*

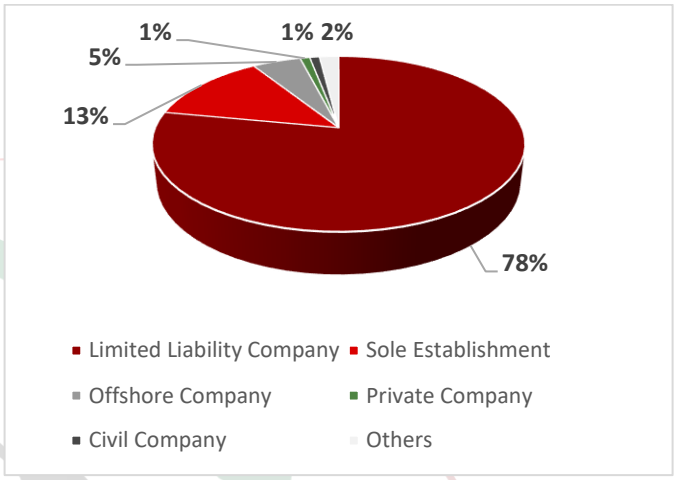


C. Money laundering through Trading System

1. Abuse of Legal Person Bank Account

Although legal persons play a significant role in the global economy, criminals often employ corporate vehicles [17] with complex legal structures across borders in their modus operandi and schemes. Over the past years, the UAEFIU has closely observed the development of abusing UAE established legal persons in a variety of criminal acts. Accordingly, the UAEFIU discussed the involvement of legal persons in financial crimes, directly or indirectly, in almost all of the UAEFIU typology reports.

CHART 3–*Legal form of examined entities in a sample of (819) STRs/SARs*



The following are the most commonly observed typologies:

- *Using Front or Shell Entities in Illegal Activities*

The typical pattern usually 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 would 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.

An increasing trend is observed in newly established companies receiving high turnover who have a business nature that is not expected to have

[17] 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

a large amount of inflow and outflow of funds in a short period of time. The entity's owner is noted in different scenarios to have no business background or seems to be unfamiliar with the established entity's business activities.

- *Complex Offshore Structure*

The offshore structure is noted to be used as a vehicle through which to move suspicious funds, particularly in the purchasing of assets on behalf of third parties or criminal networks. Subject offshore companies mainly intended to conceal a beneficial owner(s) subject to sanctioning 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 offences prosecuted abroad.

- *Major Risk Indicators*[18]

- A legal person 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 ultimate beneficial owner UBO(s).
- A legal person registered under a misleading name indicates different activities from what the business activity is licensed to practice.
- A legal person'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.
- A legal person or any of its controlling persons or affiliates is associated with a high-risk or sanctioned jurisdiction, individual or entity.
- A legal person frequently or unnecessarily changes shareholders, increases capital, and changes its business name without an obvious rationale.
- 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.
- 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.
- The circulation of funds between multiple legal entity accounts or between 'unrelated' parties in different lines of business.

2. Trade-Based Money Laundering (TBML)

The abuse of legal entities in money laundering schemes usually involves TBML techniques in different schemes to integrate illicit funds with the international trading system and conceal the identity of the beneficial owner. As indicated by the FATF: "The UAE banking sector is at increased risks of TBML."[19] As a result, TBML has been a focus area of the UAE National Action Plan. **The UAEFIU identified the most common patterns of legal persons misusing their accounts as well as TBML techniques involving the UAE financial system, as follows:**

- *The Use of Back-to-Back Letters of Credit (LoC)*

These are commonly used as a guarantee to finance trade transactions in a three-party agreement including a seller, buyer and intermediary. These consist of two distinct LoCs — one LoC issued by the buyer's bank with the intermediary as the

[18] For further risk indicators, please review the UAEFIU report 'The Abuse of Legal Persons and Arrangements in Illicit Activities', issued in March 2023.

[19] FATF (2020) 'Anti-money laundering and counter-terrorist financing measures: UAE mutual evaluation report', p.28.

beneficiary, and another LoC issued by the intermediary in favor of the seller (claimable upon fulfillment of the contract's terms and conditions). The most observed pattern in the UAE in relation to this method usually involves a shipment backed by LoCs that are genuine but whose supporting documents are not. Another common pattern involves goods being released before the offshore bank can present the bill of lading to the buyer's bank.

- *Presentation of Fictitious Documents*

A common pattern in this technique comprises discrepancies in supporting documents, particularly invoices and bills of lading. Shipments would be supported by bills of lading that are not verifiable through the International Maritime Bureau (IMB). The aforementioned discrepancies include, but are not limited to, the wrong vessel or ship, a missing chassis or container number, the wrong dates, an incorrect description of shipment, incorrect parties, spelling mistakes, and non-matching with the invoice. The supporting documentation might also be completely fake or plagiarized.

- *Phantom Shipment*

In this scheme, two parties collude with each other, and supporting evidence (like fake invoices and transportation documents) is created dishonestly. The seller sends all of the supporting documents to the buyer of goods which may not essentially exist or be dispatched. In return, the same buyer makes the payment against the sham goods.

- *Over-Invoicing/Under-Invoicing*

Over-invoicing or under-invoicing is concerned with misrepresentation of the price of goods to be traded. Over-invoicing concerns shipping goods at a higher price than their market value; thus, the buyer is transferring high economic value to the seller (i.e., advantage to the seller). Over-pricing is usually common in cases of tax evasion. Conversely, under-invoicing is concerned with shipping goods at a lower price than their market value; hence, the buyer is transferring lower economic value to the seller (i.e., advantage to the buyer). This pattern has been shown in STRs as well as requests received from the UAEFIU's international counterparties.

Ultimately, many legal entities involved in TBML showed complex ownership structures, with local entities collaborating with foreign ones (e.g., holding companies). In such a case, the legal entity in the UAE received multiple wire transfers from a legal entity in a foreign jurisdiction and then 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 possible abuse of LPs in the UAE to bypass/receive funds related to tax evasion, among others, through the use of TBML techniques.

- *Major Risk Indicators*[20]

- The corporate structure of a trade entity appears to be unusually complex and illogical, such as

[20] For further risk indicators, please review the UAEFIU report 'Trade-Based Money Laundering' issued in 2021.

involving shell companies or companies registered in high-risk jurisdictions.

- A trade entity lacks an online presence, or the online presence suggests business activity inconsistent with the stated line of business (e.g., the website of a trade entity contains mainly boilerplate material taken from other websites, or the website indicates a lack of knowledge regarding the particular product or industry in which the entity is trading).
- A trade entity displays a notable lack of typical business activities (e.g., it lacks regular payroll transactions in line with the number of stated employees, transactions relating to operating costs, tax remittances).
- A trade entity maintains a minimal number of working staff, inconsistent with its volume of traded commodities.
- The name of a trade entity appears to be a copy of the name of a well-known corporation or is very similar to it.
- A trade entity engages in complex trade deals involving numerous third party intermediaries in incongruent lines of business.
- A trade entity engages in transactions and shipping routes or methods that are inconsistent with standard business practices.
- A trade entity makes unconventional or overly complex use of financial products (e.g., the use of letters of credit for unusually long or frequently extended periods without any apparent reason; the intermingling of different types of trade finance products for different segments of trade transactions).
- Inconsistencies across contracts, invoices or other trade documents (e.g., contradictions between the name of the exporting entity and the name of the recipient of the payment; differing prices on invoices and underlying contracts; or discrepancies between the quantity, quality, volume or value of the actual commodities and their descriptions).
- Contracts, invoices or other trade documents display fees or prices that do not seem to be in line with commercial considerations, are inconsistent with the market value, or significantly fluctuate from previous comparable transactions.

D. Professional Money Laundering and DNFBPs

Professional money laundering (PML) is known as the facilitation of money laundering services on behalf of criminals or criminal groups for a fee. PML is conducted by professionals, namely an individual professional or in a form of group or network, who usually engage in sophisticated money laundering schemes to enable criminals to obtain a veneer of legitimacy on their illicit proceeds while evading AML/CFT measures. They usually operate on a large scale that could also be a subset of third party launderers.

PML is most often tangled with the establishment of front/shell entities, cash couriers and money mules, hawala providers, consultancy companies, and virtual currencies, and has a strong association with DNFBPs.

Data analysis of different samples of suspicious reports illustrated that the UAE is used as a pass-through to route or layer unknown sources of funds with the assistance of DNFBPs. DNFBPs might also act as intermediaries that facilitate transactions or invoice settlement.

The most observed legal forms employed by DNFBPs in reported suspicious activities are '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.'

A 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.

DNFBPs' transactions often involved different counterparties in foreign jurisdictions receiving or sending transfers, while not being disclosed in the KYC, and the DNFBPs failed to provide genuine documents with which to substantiate their relationship with them. DNFBPs' personal account could also be used to receive a high value of inward remittances from the same third parties. **The following are snapshots of common relevant patterns *directly* involving DNFBPs:**

- *Dealers in Precious Metals and Stones (DPMS)*

The most common patterns noted involving DMPS in suspicious criminal acts included the following: employing multiple cash couriers acting on behalf of frequent DPMS in importing cash into the country (possibly a 'cash courier network'), as well as misusing DPMS entities to import and export cash on behalf of another legal person or an exchange house.

Moreover, 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, and the possible proceeds from selling this gold were routed through multiple entities' accounts in the UAE.

- *Real Estate Professionals*

One of the common patterns observed in suspicious reports involving real estate is that of possible witting involvement of a broker acting as a third party on behalf of a criminal abroad. The UAE financial institution customer's (broker's) account would receive significant (unknown) cash deposits and inward remittances from a party who was found to be a subject of imprisonment abroad, criminal procedures, and fraudulent schemes, among others. Said funds would then be sent to the customer's other accounts in other financial institutions and toward different real estate projects and firms. Thus, the broker would be acting as a third party in moving and concealing the criminal proceeds to be integrated into the real estate sector.

In cases in which a real estate firm is the subject of a STR, intensive transactional routing behavior is noted among different real estate firms (local or foreign) as well as individuals through multiple inward and outward remittances and many cheque deposits and withdrawals.

- *Company Service Providers (CSPs)*

Bank accounts would be used directly or controlled by gatekeepers in more sophisticated transactions, e.g., fraud operations. 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. The most observed pattern in relation to CSPs is the misrepresentation and omission of critical information by colluding with the criminal, as well as providing false information to the financial institution.

- *Major Risk Indicators*[21]

- An individual sets up multiple companies dealing in different lines of business simultaneously.
- The circulation of funds between several entities' accounts without any apparent reason, who might also be suspected of being shell or front companies.
- Transactions involving 'gatekeepers' are found to have no rationale nor apparent reason, especially to engage in several investments and purchase assets (specifically high-value items).
- Funds received from an offshore party are subsequently routed to different personal or business accounts.
- A group of customers use similar contact information with an unreasonable explanation (e.g., address, mobile number, email address).
- The account holder is suspected of acting on behalf of a third party but not disclosing that information or is being controlled by someone else.

E. Closer look at DNFBPs' High Sectoral Risk Involving Financial Institutions

1. Dealers in Precious Metals and Stones (DPMS) Links with FIs

Precious metals and stones (PMS) are attractive to criminals and terrorists because they offer a high level of liquidity and anonymity, in addition to having a compact size (so they can easily be stored or smuggled). Given the UAE's inherent risk as a global financial center and trade hub, as well as its cash-intensive economy and its significant contribution to PMS global trade, the risk of this sector being abused is high.

- *Trade-Based Money Laundering (TBML) by DPMS Entities*

The establishment of dealers in precious metals and stones (DPMS) entities as a '**front**' is a common typology of laundering illegal proceeds and usually involves using TBML methods such as false invoices, phantom shipments, and fictitious sales agreements/contracts. DPMS are possibly exploited to transfer/move foreign illegal proceeds through the financial system in the country disguised as trade-based activities. This is in addition to the use of multiple DPMS entities (i.e., network) to facilitate the 'layering' of funds, basically by sending/receiving large wire transfers or remittances to/from multiple local or international counterparties, and then circulating the funds amongst domestic entities with no apparent justification for such proceeds or movement.

- *Money Laundering through 'Foreign Currency Exchange' by DPMS Entities*

DPMS entities might instruct individuals (who might be employees, representatives or external parties) to undertake '**foreign currency exchange**' (FOREX) services on behalf of the entity without involving the name of the DPMS entity in such transactions in

[21] For further risk indicators, please review the UAEFIU report 'Professional Money Laundering and Foreign Proceeds of Crimes' issued in 2021.

order to conceal the actual source of cash. When the amount exchanged exceeds the threshold, another individual will continue with the transaction to avoid the detection and documentation requirements. Some individuals involved in this trend stated that the source of funds was that of either 'salaries' or 'savings,' while the purpose was that of **'family maintenance'** or '**travel**.'

In another pattern, the DPMS entity (under its name) conducts large FOREX transactions without justification or sufficient documentation to substantiate the volume of activity as well as the source of cash. Such entities would be connected with a high value of cash imports and exports on a frequent basis. Moreover, the purpose of these transactions usually stated by the entity is either: (1) to pay suppliers who only accept cash as a payment method, or (2) to pay suppliers via cash in another jurisdiction (cross-border cash movement).

- *Major Risk Indicators*[22]
- DPMS entity has a peculiar structure that is unreasonable and complex, e.g., there is potential involvement of shell companies, a parent or subsidiary of an offshore company, in which the UBO is difficult to identify or cannot be identified.
- The circulation of funds between multiple DPMS accounts, or between 'unrelated' parties which are in different lines of business.
- Large and complex transactional behaviors for newly established entities as DPMS.
- Unnecessarily maintaining multiple bank accounts for the same entity (DPMS), or opening accounts under the names of employees.
- The transaction structure appears to be unnecessarily layered and designed to obscure the true origin of funds.
- Transactions in a DPMS account(s) are seemingly of a pass-through nature, with funds directly debited via wire transfers leaving a low balance in an account.
- DPMS or its representatives fail to provide a 'customs declaration' in relation to a local/foreign currency cash deposit related to buying/selling precious stones.
- DPMS entity engages in transactions and shipping routes or methods that are inconsistent with standard business practices.
- Contracts, invoices, or other trade documents provided by a DPMS have vague or missing descriptions, or appear to be counterfeit.
- DPMS entity or any of its counterparties appear to import precious metals and stones that originate from a country in which there is limited production or no mines at all.
- DPMS entity that is heavily engaged in cross-border cash movement.
- DPMS entity and its associates, or multiple individuals (external parties), excessively conduct foreign exchange transactions (FOREX) without any business rationale.
- Payment for imported PMS is made by an entity other than the consignee for no clear business reason, e.g., by a shell or front company not involved in a trade transaction.

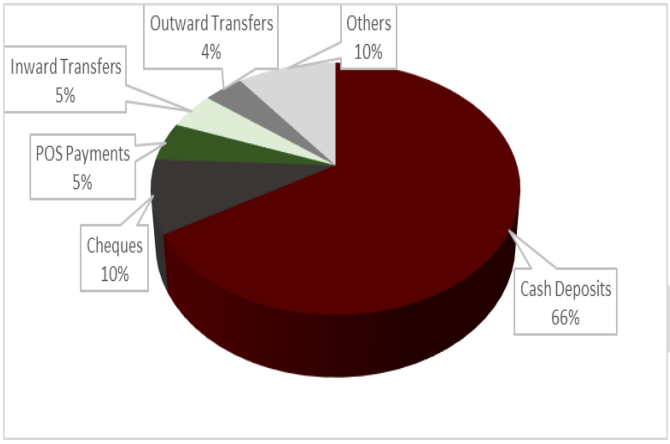
[22] For further risk indicators, please review the UAEFIU report "Dealers in Precious Metals and Stones" issued in October 2022.

2. Integration of Illicit Funds into UAE Real Estate through FIs

Real estate sector has always been attractive to money launderers because it facilitates the integration of criminals' ill-gotten proceeds through, for example, accessing the financial sector, startup businesses, and justifying large capital flows across borders.

The most noted frequent mode of transaction used in real estate payments is cash deposits, followed by cheques, POS payments, internal transfers, and outward transfers. Cash deposits consist of deposit transactions conducted through ATMs and over the counter (most frequent). Cheques entail all types of cheques, such as manager cheques and clearing cheques, regardless of whether they are deposits or withdrawals.

CHART 4: *Mode of transactions employed in real estate payments*



The main observed patterns of abusing the financial sector to integrate ill-gotten funds into the real estate sector include the following:

- *The Use of Third Parties and Family Members*

One of the frequent patterns of integrating ill-gotten funds via the real estate sector involves depositing structured amounts of funds to be funneled in buying a property, which consists of using a third party (customer) on behalf of the funds/property beneficiary. The customer might have power of attorney (POA) or a signed sale and purchase agreement with different individuals or alleged investors abroad who do not have bank accounts in the UAE. The customer's account usually witnesses the receipt of significant cash or cheque deposits (including cash deposits through ATMs in different locations by different subjects). Subsequently, the credited funds would be utilized through manager cheques (issued from different branches or multiple FIs) and/or credit cards toward purchasing a property, in addition to outward remittances to different individuals or entities, leaving no or a low balance in the account.

Another observed pattern involves a group of individuals' mules opening personal banking accounts for salary purposes. The new accounts would not witness salary-related transactions, but rather would be used with corporate accounts to receive structured cash deposits as well as inward internal transfers and remittances (whether through banking accounts or MSBs). Inward remittances might involve foreign accounts and be routed among the group members. Subsequently, the funds are utilized through cash withdrawals and outward internal transfers and remittances within a relatively short period of time.

Within the context of abusing legal structures, a common pattern is observed in which accounts of different natural and legal persons show layering and routing patterns of a series of complex transactions among multiple counterparties,

whereby suggesting possible involvement of legal persons as front/shell companies for unknown third parties. The transactional routing pattern, especially with multiple foreign entities in different jurisdictions, implies the possibility of money laundering for the benefit of a more extensive network or organized crime group. Ultimately, financial institutions' accounts are used by third parties to route transactions on behalf of the ultimate beneficial owner through the purchase of properties in the UAE.

- *Claimed Rental Income*

A frequently identified pattern consists of a customer receiving a high volume of cash and/or cheque deposits, followed by outward remittances and/or POS transactions toward installments of real estate properties. Cash and cheque deposits in such cases are justified as rental income or in selling properties in a short period of time (where the customer usually owns different properties abroad). In typical cases, there would not be sufficient evidence to support such a claim. However, many scenarios highlighted the employment of suspected counterfeit and fabricated documents.

- *The Use of Mortgages and Early Settlement*

Different STRs indicated the use of a long-term home finance agreement between the financial institution and the customer to then be settled in a short period of time. For example, the loan would be funded through manager cheques or inward remittances from the customer's own (front/shell) company account to settle and close the loan early. The loan would be settled in a few months following obtainment of the loan through one or multiple payments.

Further data from STRs suggested the possibility of individuals paying home finance shortly after obtaining the loan through unlicensed hawala service providers or unrelated legal persons licensed as wholesalers.

Such a pattern could indirectly involve foreign PEPs using family members and third parties through a complex structure of legal persons who would lend a high amount of funds under alleged loans to a counterparty (legal person). The counterparty (as a recipient of the loans) would utilize them in purchasing multiple residential properties under the corporate name.

- *Manipulation of Property Price*

The property would be sold to the customer at a significantly lower or higher price than the purchase price. The amount is often paid through manager cheques, which usually alert the financial institution's monitoring system. Such a pattern could also be observed through a non-resident buying a property by issuing POA to a broker and contacting the same broker in a short period of time to sell the property.

In this identified pattern, the employment of fabricated-price documents was frequently observed.

- *Unlicensed Real Estate Crowdfunding*

The transactional pattern would involve an individual account receiving multiple ATM cash deposits, manager cheques, and transfers from own accounts and other individuals. The inward funds would be followed by cash withdrawals, manager cheques toward properties, and outward transfers to multiple individual counterparties and own accounts. In such a scenario, the customer collects funds from multiple individuals to buy a

property under his/her name and then pays back the involved individuals with (investment) profit from selling the property. The same customer might also transfer funds to other individuals to buy properties under their names and then receive funds from them as profit.

- *Major Risk Indicators*[23]

- A customer's account transactions resemble purely a mule account's activities for third parties.
- A high volume of anonymous funding into the account from multiple unknown individuals and/or entities.
- An internal self-transfer from the customer's other accounts abroad with no supporting documents on the source of funds.
- Substantial remittances in a short period of time from a family member(s) abroad to be utilized in real estate in the UAE.
- A payment service provider pays on behalf of an offshore company to purchase multiple properties in the UAE.
- Customer accounts receive significant amounts of cash deposits and/or inward remittances from unknown parties to be utilized in property purchases or installments.
- Credits into an individual account are only noted as manager cheques, while there is no information on the ultimate remitter of these funds and the beneficiary of the property.
- Funds are transferred to settle a credit card, followed by installments to purchase a property on behalf of a friend.
- Funds received are immediately spent whilst conducting various card payments toward real estate purchases or installments.
- An individual account seems to be used as a funnel account through receiving multiple unknown deposits and remittances for real estate crowdfunding.
- A company (third party) lends or pays for a customer's property price while having no direct relation with the customer (borrower).

F. Other High-Risk Vulnerabilities: Circumvention Sanction

Different samples of suspicious reports indicated the abuse of legal persons as a vehicle through which to route transactions on behalf of a sanctioned entity or third party. Most observed legal persons for potential circumvention sanction evasion were limited liability companies (LLCs) established in free zones and also on the mainland, practicing various codes of activity, but mainly general trading of different goods and items, as well as consultancy firms.

Data analysis also illustrated 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. Newly established entities are most often the subject of reported suspicious activities in this regard, but also entities that have been subject to multiple changes in shareholders, directors and business activities, in an attempt to hide or avoid the tracking of illicit activity back to their ultimate controller.

[23] For further risk indicators, please review the UAEFIU report 'Real Estate Money Laundering Typologies and Patterns' issued in December 2023.

A commonly observed transactional pattern is that of 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, as well as abusing trading chains to move funds, including TBML techniques. 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 legal persons for sanction evasion purposes involves a legal person being 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. Abuse of a legal structure directly or indirectly established by a subject of circumvention sanctions was also observed through the establishment of multiple (shell) entities, including real estate firms to move and integrate funds using corporate bank accounts and the real estate sector.

This report is produced by the UAEFIU-Research and Strategic Analysis Section. For inquiries and communication, please contact

rsas@uaefiu.gov.ae