



Guidance on Suspicious Transactions Reports (STRs) / Suspicious Activity Reports (SARs) and Red Flag Indicators

For Designated Non-Financial Businesses and Professions (DNFBPs)



Table of Contents

1.	Introduction	3
1.1.	Purpose and Scope	3
1.2.	Legal Status	3
2.	Understanding STRs & SARs	4
2.1.	Suspicious Transaction Reports (STRs)	4
2.2.	Suspicious Activity Reports (SARs)	5
3.	Timing of STR/SAR Reporting	5
3.1.	Filing Reports Without Delay	5
3.2.	High-Risk Scenarios	5
4.	Internal Governance & Controls	5
5.	STR/SAR Content, Quality & Post-Submission Obligations	6
5.1.	Essential Elements of the Report	6
5.2.	Narrative Reporting	6
5.3.	Reasons for Reporting (RFRs)	7
5.4.	Handling of Transactions and Business Relationships after Filing of STRs	7
6.	Confidentiality and Prohibition against "Tipping Off"	7
7.	Record Keeping	8
8.	Other Key Considerations	8
9.	Red Flag Indicators	8
9.1.	Red Flag Indicators for REAB	9
9.2.	Red Flag Indicators for DPMS	12
9.3.	Red Flag Indicators for TCSPs	16
9.4.	Red Flag Indicators for IAAs	19
10.	Annexure I – Other Report Types	23



Introduction

This Guidance is issued by the Ministry of Economy and Tourism (MoET) to assist Designated Non-Financial Businesses and Professions (DNFBPs) with understanding and effectively fulfilling their regulatory obligations regarding the identification and reporting of suspicious transactions and activities, as defined under the Anti-Money Laundering, Counter-Terrorism Financing and Counter Proliferation Financing (AML/CFT/CPF) framework of the United Arab Emirates (UAE).

Suspicious Transaction Reports (STRs) / Suspicious Activity Reports (SARs) serve as crucial tools in the identification, prevention and disruption of money laundering (ML), terrorist financing (TF), proliferation financing (PF) and the funding of illegal organizations. Serving as a pivotal source of financial intelligence, the quality, timeliness and analytical value of STRs/SARs is of the utmost importance for the effectiveness of the national AML/CFT/CPF regime.

Under the UAE AML/CFT/CPF legal and regulatory framework, DNFBPs are required to promptly report suspicious transactions and any additional information where there are suspicions, or reasonable grounds to suspect that proceeds are related to a crime, or to the attempt or intention to use funds or proceeds for the purpose of committing, concealing, or benefitting from a crime.

Failure to comply to this reporting mandate, whether intentionally or by gross negligence, constitutes a regulatory violation and may result in administrative sanctions, as prescribed in the AML/CFT/CPF Law. Where failure to report involves the deliberate concealment, collusion or participation in ML/TF/PF or tipping off, criminal liability may be incurred under the governing legal framework. This liability applies to the DNFBP, its senior management or employees who fail to perform their statutory obligation to report a suspicion of ML/TF/PF and related predicate offences.

1.1. Purpose and Scope

The purpose of this Guidance is to establish clear supervisory expectations regarding STR/SAR reporting and support DNFBPs adhere to their statutory obligations under the legal and regulatory framework in force in the UAE.

This Guidance is not intended to limit, replace or otherwise affect the applicability of additional or supplementary guidelines, circulars, notifications, memoranda, communications, or other forms of guidance or feedback (whether direct or indirect) that may be published periodically by any relevant authority in relation to regulated entities within the respective jurisdictions, or to any specific regulated entity.

Unless otherwise noted, this Guidance applies to all DNFBPs, and the members of their boards of directors, management and employees, established and/or operating in the territory of the UAE and respective Free Zones. More specifically, and without prejudice to the definition of a DNFBP, as provided for in the relevant legislative and regulatory framework of the UAE, this Guidance applies to:

- Real Estate Agents and Brokers (REAB)
- Dealers in Precious Metals and Precious Stones (DPMS)
- Independent Accountants and Auditors (IAA)
- Trust & Corporate Service Providers (TCSP)

Note: DNFBPs should refer to the full TFS guidelines issued by the Executive Office for Control and Non-Proliferation (EOCN), which detail obligations under *Cabinet Decision No. (74) of 2020*, including requirements for screening, freezing, and reporting in relation to designated persons or entities.

1.2. Legal Status

Under federal law and regulations, whether the DNFBP operates in the UAE mainland or Financial or Commercial Free Zone, the designated competent authority for receiving reports of suspicious transactions or activity is the UAE Financial Intelligence Unit (FIU). Placing indicators to identify suspicious transactions / activities, reporting suspicious transactions / activities to the FIU and cooperating with relevant authorities, inclusive of non-disclosure of information or data in an STR/SAR are the minimum statutory obligations that apply to DNFBPs under the UAE's AML/CFT/CPF Law.



This Guidance serves as a practical tool to assist regulated DNFBP entities in adhering to reporting mandates and is intended to be read in conjunction with the relevant laws, cabinet decisions / resolutions, regulations and regulatory rulings which are currently in force in the UAE. This Guidance does not constitute additional legislation or regulation, and is not intended to set legal, regulatory, or judicial precedent. Regulated entities are reminded that the Guidance does not replace or supersede any legal or regulatory requirements or statutory obligations. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail.

Specifically, nothing in this Guidance should be interpreted as providing any explicit or implicit guarantee or assurance that the Supervisory or other Competent Authorities would defer, waive, or refrain from exercising their enforcement, judicial, or punitive powers in the event of a breach of the prevailing laws, regulations, or regulatory rulings.

This Guidance, and any lists and/or examples provided in it, are not exhaustive and do not set limitations on the measures to be taken by regulated DNFBP entities to meet statutory obligations under the legal and regulatory framework currently in force. As such, this Guidance should not be construed as legal advice or legal interpretation. Regulated DNFBP entities should perform their own assessments of the manner in which they should meet statutory obligations and should seek legal or other professional advice if they are unsure of the application of the legal or regulatory frameworks to circumstances.

2. Understanding STRs & SARs

2.1. Suspicious Transaction Reports (STRs)

Under the pertinent AML/CFT/CPF Law and AML/CFT/CPF Decision, a suspicious transaction refers to any transaction, attempted transaction, or funds for which a DNFBP has reasonable grounds to suspect as constituting in whole or in part, and regardless of the amount or the timing any of the following:

- The proceeds of crime (money laundering and related predicate offenses or financing of terrorism or illegal organisations or proliferation financing)
- Being related to the crimes of money laundering and related predicate offences, the financing of terrorism or illegal organisations or proliferation financing
- Being intended to be used in an activity related to such crimes

The AML/CFT/CPF Law defines a predicate offence as *“any act constituting a felony or misdemeanour, including the financing of terrorism, the proliferation financing, and evasion of direct and indirect taxes, in accordance with the applicable legislation of the State, whether committed within or outside the [UAE], provided that such an act is punishable in both countries”*.

DNFBPs must note that the only requirement for a transaction to be considered as suspicious is “reasonable grounds” in relation to the conditions referenced above. Thus, the suspicious nature of a transaction can be inferred from certain information, including indicators such as transactional and behavioural patterns, Customer Due Diligence (CDD) information and/or adverse media information, and it is not dependent on obtaining evidence that a predicate offence has occurred or on proving the illicit source of the proceeds involved.

DNFBPs do not need to have knowledge of the underlying criminal activity nor any founded suspicion that the proceeds originate from a criminal activity; reasonable grounds to suspect any such criminal activity are sufficient. DNFBPs should also note that suspicious transactions need not be completed, in progress, or pending completion. Attempted transactions, transactions that are not executed and past transactions, regardless of their timing or completion status, which are found upon review to cause reasonable grounds for suspicion, must be reported in accordance with the relevant requirements.

Where a DNFBP has reasonable grounds to suspect that a transaction (completed, ongoing or attempted) involves the proceeds of crime and/or lacks an apparent lawful or economic purpose, a suspicious transaction report must be submitted to the FIU via the goAML portal.



2.2. Suspicious Activity Reports (SARs)

Conversely, while an STR stems from suspicions around transactional conduct, a suspicious activity report (SAR) arises from non-transactional conduct which includes customer behaviour, attempted misuse of DNFBP services, or adverse information identified at any of the following stages:

- Prior to onboarding where suspicious indicators arise (e.g. falsified documents, reluctance to provide information required as part of due diligence)
- During onboarding whereby adverse information or unusual behaviour is noted
- Through ongoing monitoring where no transactions exist but behaviour, declarations, screening outcomes raise suspicion.

To reiterate, Suspicious Activity Reports enable DNFBPs to alert the FIU on non-transactional behaviour and contextual risk-based concerns which include, but are not limited to, potential misuse of services, suspicious attempts, adverse media findings, unusual customer conduct and/or falsified/inconsistent information provided that give rise to reasonable grounds for suspicion. SARs involve details on the customer and a narrative of suspicion without full transactional data, relative to STRs which require full transactional data and related supporting documents. Where adverse media is the trigger for reporting, supporting document i.e. screening results are to be submitted with the report. It is important to note that the rule of thumb in relation to "reasonable grounds" as prescribed in *Section 2.1* remains unchanged when deciding to file SARs.

3. Timing of STR/SAR Reporting

3.1. Filing Reports Without Delay

DNFBPs are expected to file reports in a timely manner in order to preserve the operational value of financial intelligence. Thus, DNFBPs must demonstrate effective mechanisms of escalating suspicions through clearly defined channels, completing assessments of referrals expeditiously and submitting STRs/SARs once reasonable grounds have been established.

Delays without proper justification, failure to escalate suspicions or batching of reports are inconsistent with supervisory expectations and may result in the applicable enforcement actions.

3.2. High-Risk Scenarios

Instances with indicators that involve terrorist financing and targeted financial sanctions (TFS) should prompt for immediate reporting and the application of appropriate measures, as prescribed in the applicable guidelines.

Additionally, requests or enquiries from competent authorities are to be considered of utmost importance and should be addressed without delay.

4. Internal Governance & Controls

DNFBPs must demonstrate sound governance structure in order to be able to effectively monitor and identify unusual or potentially suspicious activity and submit timely reports. This entails the design and implementation of core elements related to an effective compliance program: management oversight, policies and procedures which govern the DNFBP's onboarding, ongoing monitoring processes, clear lines of responsibility and reporting, training, compliance monitoring and assurance.

Business & Operational Level – First Line of Defence (FLoD)

Customer-facing employees, business, operational and support functions play an important role in the identification of potentially suspicious transactions and/or activities due to direct exposure that enables the detection of unusual behaviour, inconsistencies or risk indicators. These indicators may be picked up on at the time of direct interaction with customers or during review of documentations. DNFBP employees performing functions at this level must be able to understand ML/TF/PF risks, understand regulatory obligations, recognize red flags and identify inconsistencies between a customer's declared profile and behaviour, apply appropriate risk mitigation measures and escalate matters that give rise to reasonable grounds for suspicion in line with the defined escalation matrix.

Compliance Level – Second Line of Defence (SLoD)

The onus of independent oversight, guidance and review of referrals pertaining to suspicions lies with the DNFBP's Compliance Function. While suspicions are reviewed, documented and escalated



by FLoD, the ultimate decision to file STRs/SARs must be taken by the DNFBP MLRO/Compliance Officer. In this regard, the MLRO/Compliance Officer is responsible for the:

- Assessment of escalations received from FLoD in a manner that is objective and independent of any influence
- Documentation of decision to file or not file STRs/SARs with appropriate justification
- Oversight over the suspicious activities / transactions identification and reporting processes
- Adherence to applicable AML/CFT/CPF laws and regulations
- Reporting of ML/TF/PF risk exposures and STR/SAR/CNMR/PNMR¹ trends to senior management

Independent Testing Level – Third Line of Defence (TLoD)

The evaluation of design and operational effectiveness of the DNFBP's compliance program should be undertaken by an independent testing function. This testing should be conducted by an internal audit department, external auditors/consultants and/or other qualified independent third parties in a manner that is risk-based to be able to identify deficiencies and ensure appropriate remediation plans are in effect to address those deficiencies.

Risk-Based Monitoring

DNFBPs must demonstrate appropriate monitoring and risk mitigating measures that are proportionate to the nature, size and complexity of their business operations as well as proportionate to the ML/TF/PF risks associated with their business activities. These measures should support timely detection of unusual or potentially suspicious activities and should consider various aspects of the DNFBP's dealings, such as (but not limited to):

- Cash-based transactions
- Association of high-risk jurisdictions and/or high-risk customers
- Unusual patterns of behaviour inconsistent with the customer's known profile, business or expected activity
- Unjustifiable changes to transaction behaviours, terms and conditions of dealings, ownership arrangements or counterparties

DNFBPs must conduct periodic reviews of their monitoring measures to ensure they remain appropriate and proportionate to the risks posed and nature of business operations and do not inadvertently exclude or suppress potentially reportable activities. DNFBPs must remain aware of changing risk and regulatory landscapes to make appropriate changes to their monitoring systems (whether manual or automated). Any changes to monitoring systems must be documented clearly and approved by the Compliance Officer or Senior Management.

5. STR/SAR Content, Quality & Post-Submission Obligations

5.1. Essential Elements of the Report

STRs/SARs must clearly address the following:

WHO <i>is involved</i>	WHAT <i>activity is suspicious</i>	WHEN <i>the activity occurred</i>	WHERE <i>the activity took place</i>	WHY <i>it is suspicious</i>	How <i>the suspicion was identified</i>
---------------------------	---------------------------------------	--------------------------------------	---	--------------------------------	--

DNFBPs are expected to provide documentary evidence of the facts which includes all documentation regarding the persons/entities involved as well as any documentation uncovered during internal investigations and analysis. Furthermore, DNFBPs are expected to explain what actions have been taken in light of the reported incident. Detailing the investigative and analytical steps taken as well as outcomes actions aside from the raising of the report to the FIU.

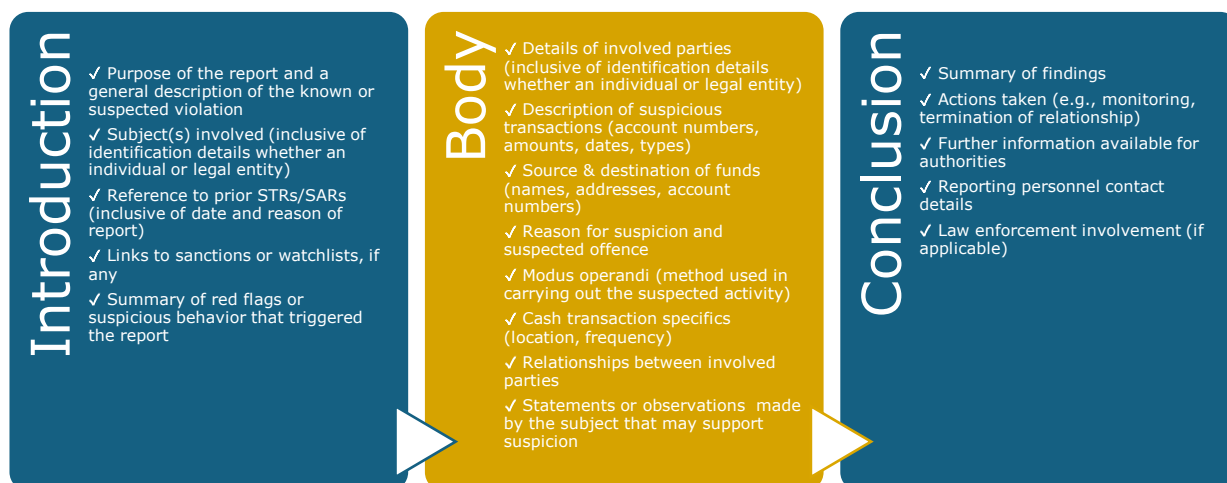
5.2. Narrative Reporting

When all relevant information has been collected, analysed, and documented, and the DNFBP entity determines that an STR or SAR is warranted, the details must be presented in a concise, chronological format using a similar narrative report template as provided in the diagram below

¹ CNMR – Confirmed Name Match Report
PNMR – Partial Name Match Report



which presents a summary of the required narrative structure. It serves as a guide for formatting purposes but is not a substitute for the complete reporting content. The narrative report serves as a supplement to the goAML submission, addressing any limitations in the standard report description field.



5.3. Reasons for Reporting (RFRs)

When filing reports via the goAML portal, DNFBPs must differentiate between the type of report to be selected i.e. STR/SAR versus TFS (CNMR/PNMR) or threshold-based reports (REAR/DPMSR)². DNFBPs must also select the RFRs that accurately reflects the underlying suspicion³. DNFBPs must ensure that RFRs are supported by the narrative in the report and are aligned with the facts of the case.

5.4. Handling of Transactions and Business Relationships after Filing of STRs

Once STRs/SARs have been filed or other suspicious information related to a customer or business relationship has been reported to the FIU, the following two immediate actions should take place:

- DNFBPs must follow instructions, if any, of the FIU in relation to both the specific transaction and to the business relationship in general.
- The customer or business relationship should immediately be classified as high-risk and appropriate risk-based enhanced due diligence and ongoing monitoring procedures should be implemented in order to mitigate the associated risks. It is however not required to terminate the relationship unless the associated risks cannot be mitigated.

6. Confidentiality and Prohibition against "Tipping Off"

When reporting suspicious transactions to the FIU, DNFBPs are obliged to maintain confidentiality with regard to both the information being reported and to the act of reporting itself, and to make reasonable efforts to ensure the information and data reported are protected from access by any unauthorized person.

As part of their risk-based AML/CFT/CPF framework, and in keeping with the nature and size of their businesses, DNFBPs, and their foreign branches or group affiliates where applicable, should establish adequate policies, procedures and controls to ensure the confidentiality and protection of information and data related to STRs/SARs. These policies, procedures and controls should be documented, approved by senior management, and communicated to the appropriate levels of the organisation.

DNFBPs must ensure that all relevant information relating to STRs/SARs is kept confidential, with due regard to the conditions and exceptions provided for in the law, and the guiding principles for this must be established in policies and procedures. DNFBPs need to ensure that policy and procedures are reflected in for example, appropriate access rights with regard to core systems used

² Refer to Annexure I – Other Report Types

³ Selection of multiple RFRs is permissible for, where justified.



for case management and notifications, secure information flows and guidance/training to all staff members involved. This guidance is primarily important for first-line staff who have contact with customers. It is essential that customer-facing staff know when there may be cases of suspicious transactions / activities, what questions to ask the customer and which information they must not, under any circumstances, disclose to the customer.

It should be noted that the confidentiality requirement does not pertain to communication within the DNFBP or its affiliated group members (foreign branches, subsidiaries, or parent company) for the purpose of sharing information relevant to the identification, prevention or reporting of suspicious transactions and/or crimes related to ML/TF/PF.

The AML/CFT/CPF law prohibits DNFBPs or their managers, employees or representatives, from informing a customer or any other person, whether directly or indirectly, that a report has been or will be submitted, or from disclosing any information or data contained in the report, or that an investigation is under way concerning the transaction. Any person violating this prohibition is liable to the applicable penalty.

7. Record Keeping

DNFBPs must establish and maintain comprehensive records covering all transactions, CDD documentation, business correspondence, and outcomes of any analysis performed. Records must also encompass documentation generated as part of the entity's ML/TF/PF risk assessment and mitigation processes, in accordance with the requirements set out under the AML/CFT/CPF Decision.

Records are to be retained in an orderly manner that allows for effective analysis and the tracing of financial activities. They must be sufficient to reconstruct transactions in a manner that, if required, can support investigations or be used as evidence in legal proceedings. All CDD and transactional records must be readily available to Competent Authorities upon request and without undue delay.

The minimum statutory retention period for such records is five (5) years, calculated from the latest of the following events:

- The termination of a business relationship or closure of a customer account.
- Completion of an occasional transaction where no business relationship exists.
- Completion of a supervisory inspection.
- The issuance of a final judgment by a competent judicial authority.
- Dissolution, liquidation, or termination of a legal person or arrangement.

Competent Authorities may, at their discretion, require DNFBPs to extend record retention beyond the minimum period, either for specific customers, transactions, or broader categories considered of supervisory or investigative interest.

8. Other Key Considerations

DNFBPs are expected to demonstrate continuous improvement in reporting quality, timeliness and all other STR/SAR related practices over time. DNFBPs must avoid:

- Generic or template-based narratives where there is immaterial information provided
- Selection of inappropriate RFRs
- Providing incomplete customer or ultimate beneficial owner (UBO) information
- Providing repeated transaction data without analysis
- Delayed reporting without appropriate justification
- Raising STRs/SARs on the basis of high-risk nationality alone; while this high-risk nationality increases the risks of the business relationship, this fact alone does not warrant raising STRs/SARs to the FIU

9. Red Flag Indicators

The following list of red-flag indicators for potentially suspicious activity / transactions is not exhaustive. It is important to note that the presence of one or more of these indicators does not automatically imply that a transaction involves a crime. Rather, it serves as an indication that enhanced due diligence, or further investigation may be warranted. The appointed Compliance Officer of the DNFBP should carefully assess the circumstances to determine whether the activity / transaction is indeed suspicious.



9.1. Red Flag Indicators for REAB

9.1.1. Customer Behaviour

Concealing or Disguising Identity

- The identity of the person benefiting from the transaction (the beneficial owner) is obscured or disguised, or there is reluctance to disclose the true ownership.
- There is insistence on using intermediaries (professional or informal) in all interactions without a legitimate or reasonable business explanation.
- Customer refuses or is reluctant to provide required documentation, data, or information typically needed to facilitate a real estate transaction or requests that the beneficial ownership verification be deferred until late in the transaction process.
- There is use of legal persons, foreign companies, or other complex structures to protect a person's identity or obscure their involvement in the transaction.
- Attempts to bypass sanctions screening by using layered corporate structures or frequent ownership changes.

Suspicious Behaviour or Lack of Transparency

- Customer refuses to cooperate or provide information necessary to understand the source of their funds or facilitate the transaction.
- Customer actively avoids in person meetings, face to face discussions, or other direct interaction without a legitimate reason or clear explanation.
- There is a sudden shift in the customer's behaviour or the introduction of unknown third parties during the transaction process, especially if it involves the involvement of lawyers, notaries, or financial institutions when such involvement is not typical for the transaction.
- Repeated changes in the declared beneficial owner during the transaction lifecycle without a credible explanation.
- Customer or other parties involved in the transaction show little interest in the characteristics of the property or seem unconcerned with negotiating a better price or completing the transaction quickly, without a valid reason.
- The Customer is insisting on completing and paying for a high-value property in cash and has no clear source of funds.
- Instructions routed entirely through legal representatives without valid confidentiality or legal privilege justification.
- Splitting the ownership across multiple family members or entities in order to avoid screening thresholds or sanctions controls.

Unusual Customers and High-Risk or Criminal Associations

- A foreign national with no established ties to the UAE, no business or personal interests, no clear legitimate purpose, and no economic purpose for engaging in a real estate transaction.
- Transaction seems inconsistent with the customer's socio economic, educational, or professional background.
- The Customer demonstrates little or no understanding of the purpose of the transaction.
- Customer or beneficial owner has political connections or is a Politically Exposed Person (PEP) or is linked to someone holding a prominent political or public position.
- Transactions involve individuals who are under trial, have been sentenced for crimes, or are publicly linked to criminal activities (including but not limited to corruption).
- A foreign or a domestic company is used for purchasing real estate, particularly if the company structure appears unusual or overly complex.
- Transactions involve intermediaries or complex structures (such as shell companies or trusts) with no clear purpose, designed to obscure the real parties involved.
- Customer or known associates is listed on any targeted financial sanctions list or subject to embargoes or similar measures issued by international organizations (e.g., UAE Terrorist List, United Nations).
- Transactions involve customers known to be linked to criminal activities or are under investigation or trial for crimes.
- Beneficial owner residing in a jurisdiction different from the source of funds or country of incorporation, with no clear economic rationale.
- Customers or beneficial owners linked to sectors associated with dual-use goods, sanctioned trade, or sensitive technologies.



- Transactions involving entities with opaque ownership structures linked to jurisdictions subject to UN PF-related sanctions.
- Use of properties as collateral in arrangements involving sanctioned or high-risk counterparties.

Unusual Timing or Patterns in Transactions

- The customer requests the recording of the sale of a building plot which is shortly followed by the declaration of a finished new building at the same location within an unusually short period, which may indicate an attempt to avoid regulations or hide the true nature of the transaction.
- Purchase of multiple off-plan properties followed by early resale or assignment shortly after booking.
- The parties show a strong interest in completing the transaction quickly without good cause, or there are signs of urgency that don't align with the typical pace of real estate transactions.
- A customer approaches the same real estate agent on subsequent days to buy multiple properties with no clear source of funds.
- Successive selling and buying of properties among a group of individuals in a short period, involving the purchase of a property at a lower or higher market price.
- Customer withdraws from the transaction immediately after enhanced due diligence is requested.
- Customer threatens legal action or reputational harm to discourage reporting or questioning.
- Customer attempts to influence staff to bypass internal escalation or reporting processes.

9.1.2. Transaction Behaviour

Concealing the Source of Funds

- Customer is unwilling or unable to explain the source of their funds for a property transaction.
- Funds cannot be clearly verified, or the explanation of their origin is suspicious.
- Transaction involves a significant amount of cash or virtual assets without a clear explanation or a valid source.
- Transaction involves cash equivalents like bank drafts, cashier's cheques, barer negotiable instruments, or third-party cheques without clear identification of the true payer, especially for large sums relative to the total transaction.
- Part or all the settlement is made in cash or foreign currency, and there is no valid business reason, or the buyer refuses to disclose the source of funds for unusually large transactions.

Emerging Risks

- Use of cryptocurrency for transactions: If the customer wishes to use cryptocurrency (Bitcoin, Ethereum, etc.) to complete the transaction, particularly if they are unwilling to explain the origin of the digital assets or the amount is substantial compared to the value of the property.
- Use of blockchain technology in property transactions: Property-related transactions conducted through blockchain or distributed ledger technology where the source of funds, transaction trail, or counterparties are unclear, insufficiently verified, or bypass traditional financial institutions and recognised intermediaries such as wallet-to-wallet transfers.
- Untraceable digital assets: Transactions where the source of the digital currency or assets is not substantiated by supporting documents or has no clear link to a legitimate source.
- Use of virtual agents or platforms: Transactions involving virtual agents or online platforms that lack proper regulatory oversight, especially if the parties are based in different jurisdictions with unclear legal frameworks.
- Unfamiliar or non-traditional payment methods: When customers insist on using alternative payment methods, such as digital wallets, peer-to-peer payment systems (e.g., Venmo, PayPal), or offshore bank transfers that are harder to trace.

Suspicious Use of Mortgage or Investment Schemes

- Transaction appears to involve fraudulent mortgage schemes or unusual investment schemes.
- Transaction is financed by third parties, such as individuals or non-financial institutions, without a legitimate explanation or commercial justification.



- Valuation reports issued by unfamiliar or unlicensed valuers.
- Significant discrepancies between independent valuations and transaction prices without explanation.
- Pressure on valuers or agents to adjust valuations to meet financing or transfer objectives.
- Use of family offices or private investment vehicles with unclear governance or funding sources.

Unusual Transaction Frequency or Structure

- Payments are intentionally divided into smaller amounts with short intervals between them, possibly to avoid detection or scrutiny.
- Multiple properties being bought, sold, re-sold, or exchanged simultaneously or consecutively in a short period, with unexplained or illogical changes in property value.
- Acquisition of property primarily for value storage, with no intention to occupy, lease, develop, or resell within a reasonable timeframe, particularly, where linked to high-risk customers or jurisdictions.

Suspicious Relationships and Behaviours

- Transaction involves parties like nominee shareholders or directors who have no apparent connection or questionable relationship, or the transaction generates doubts that cannot be adequately explained by the customer.
- Transaction involves family members where the transaction appears to be for the reason of concealing the beneficial ownership or source of funds and no financial rationale behind it.
- Customer exerts unusual pressure or requests the transaction be completed very quickly, possibly to avoid scrutiny.
- Parties involved in the transaction are not acting on their own behalf, possibly trying to conceal the identity of the real buyer or seller.
- Two parties (buyers and sellers) are requesting to transfer the ownership of a property with a significant lower or higher price than the market price.
- Customer declaring that the escrow account will be funded by a third-party that is not linked to the buyer.
- Payments made to developers from accounts not held in the buyer's name.

Irregularities in Contracts or Agreements

- A contract is cancelled in a manner that disregards clauses that penalize the buyer with loss of the deposit, or if the cancellation is handled in a separate document while leaving the parties in possession of the original contract.
- Repeated cancellations of off plan purchases with refund requests to different accounts or jurisdictions.
- Transactions where the name on the contract or any other details change unexpectedly or without a logical explanation, particularly if it involves a significant transfer of assets.
- Requests to backdate contracts or alter transaction dates to predate sanctions designations.

Transactions That Do Not Make Economic Sense

- Transaction value is significantly higher or lower than the market value or the real value of the property.
- Transaction results in an obvious loss for one party or seems out of line with market expectations or without a reasonable rationale (distress sale).
- Properties are sold, purchased, or exchanged multiple times within a short period, with no clear financial or business rationale.

Other Transaction Pattern Red Flags

- Transaction involves structuring to avoid detection, such as breaking large sums into smaller ones, or unusual cash payments and settlements.
- Transaction that in a way hides the identity of the buyer or the motives behind the deal.

9.1.3. Geographical Risk

- Transaction involves funds that are received from a foreign country when there is no apparent connection between the country and the customer, and/or which are received from a low-tax offshore jurisdiction or one that is considered to pose a high ML/FT/PF risk.



- Transaction involves property development in an area considered to be high-risk for economic, environmental, or other reasons.
- Use of third parties, overseas accounts, or persons or entities in countries identified as high-risk jurisdictions to send or receive funds on behalf of the buyer or seller.
- Customer requests the proceeds of a sale or rental be sent to a high-risk jurisdiction or a third party apparently unconnected to the transaction.

9.2. Red Flag Indicators for DPMS

9.2.1. Customer Behaviour

Structuring

- Customers intentionally structuring amounts to avoid identification or reporting thresholds. For example, numerous small transactions over a short period, such that each is below the regulatory threshold for the relevant level of CDD, but the cumulative total is substantial. This behaviour is also known as Smurfing.
- A customer who approaches different branches of the same DPMS in a short period to conduct transactions below the reporting threshold.
- Repeated structuring behaviour observed over time, even where individual transactions appear compliant when viewed individually, indicating a pattern that may warrant enhanced review or further assessment rather than isolated or one-off activity.
- Customers who restructure transactions or split payments shortly after being informed of applicable reporting, record-keeping, or identification requirements, which may indicate an attempt to remain below regulatory thresholds and therefore require additional scrutiny.
- A group of individuals (especially non-residents) approaching the same DPMS, conducting multiple cash transactions below the reporting threshold.

Unusual Requests & High-Risk or Criminal Association

- Sudden and unusual inquiries about refund policies, followed by requests for large refunds.
- Requests to alter or cancel a transaction after being asked for identity or supporting documents.
- A customer exhibits an unusual hurry to complete the transaction.
- Abnormal requests for precious metal conversions into ordinary objects to disguise the identification of PSPM.
- Sudden unexplained changes in the volume or value of transactions that are inconsistent with the customer's known profile.
- The customer appears related to a high-risk country, territory, or entity associated with CAHRA origin gold trading linked to money laundering or terrorism activities, or to a person designated as a terrorist.
- Potential involvement of shell companies, a parent or subsidiary of an offshore company, where the Ultimate Beneficial Owner (UBO) is difficult or impossible to identify.
- The customer is linked to negative news or criminal activities, such as being named in a news report about a crime or being under investigation by law enforcement.
- A politically exposed person (PEP) who is linked to negative news or crime, or any family member or close associate of such a PEP.
- A customer who is linked to a designated terrorist individual or organization.

Lack of Transparency or Documentation and Forgery

- The customer fails to provide sufficient explanation or documentation for the source of funds. For example, attempts to use a third-party cheque or credit card with questionable or untraceable ownership.
- The customer is unable or unwilling to provide information for due diligence and record-keeping purposes.
- Vague or refusal to provide information on the reason for buying or selling PSPM, or about the origin of the items.
- The customer is unable or unwilling to identify beneficial owners or controlling interests, where this would be commercially expected.
- The customer is suspected of using forged, fraudulent, false, or digitally manipulated identity documents for due diligence and record-keeping purposes.
- Repeated requests to modify transaction terms, documentation, or counterpart details after initial compliance review.



Secrecy and Evasion

- The customer attempts to maintain a high degree of secrecy regarding the transaction, for example:
 - Requests that normal business records not be kept.
 - Refuses to provide information for due diligence and record-keeping purposes.
- The customer is unusually concerned with reporting thresholds or the Anti-Money Laundering (AML) / Combating the Financing of Terrorism (CFT) / Counter Proliferation Financing (CPF) policies of the entity.
- Frequent changes in ownership, management, or business names without a clear business rationale.
- Customer demonstrates heightened concern about FIU reporting thresholds or internal escalation processes.

Other Behavioural Red Flags

- The customer is accompanied by others who appear suspicious, such as lurking outside the premises or closely monitoring the customer and are evasive when asked for further details.
- The customer is employed by a DPMS entity but is conducting transactions in a personal capacity.
- The customer unnecessarily self-discloses that their funds are clean and not involved in any money laundering activities.
- Sudden disengagement from a long-standing relationship when enhanced due diligence is applied.

9.2.2. Transaction Behaviour

Unusual or Complex Payment Arrangements

- Involving unusual or complex payment arrangements without an apparent legitimate business or economical purpose.
- Transaction structure appears unnecessarily layered and designed to obscure the true origin of funds.
- Transactions involving the use of stolen or fraudulent payment instruments, such as payment cards that appear stolen, altered, or not issued in the customer's name.

Involvement of Third Parties

- Transactions involving third parties as payers or recipients of payment or PSPM, without legitimate business purpose. Examples include:
 - Payments received from a third party, who is not the owner of the funds, without legitimate business purpose.
 - Payments received from multiple unrelated third parties for the same transaction.
 - Payments of proceeds made to third parties overseas, despite the transaction being between a domestic buyer and seller, with no legitimate business purpose.
 - PSPM delivered to a third party, who is not the owner or payer of funds, without legitimate business purpose.
 - Refunds paid to a third party, who is not the owner or payer of funds, without legitimate business purpose.
- Use of third-party cheques, third-party credit cards, precious metals (e.g., gold bars), precious stones (e.g., diamonds), or digital payment tokens.
- Introduction of third parties late in the transaction lifecycle without documented commercial rationale.
- Change in payer or recipient immediately following source of funds or ownership inquiries.

Suspicious Transaction Profiles or Amounts

- Transactions that are inconsistent with the usual profile of a customer, such as:
 - Transactions that appear to be beyond the customer's means based on their stated or known occupation or income, experience in the industry, or known share capital or period of incorporation.
 - Transactions that appear to be more than the usual amount or quantity for a typical customer.
 - Transaction purposes that are not aligned with the known or expected operations of the business.
- Series of transactions in different names.



- Transactions that do not consider the value, size, and/or colour of the precious stone, precious metal, or precious product.

Overpayment and Refund Requests

- Overpayment and requests for refunds of excess amounts to a third party or in cash.
- Large transactions that are cancelled shortly after deposits or full payment are made, resulting in refunds. For example, a customer may pay in cash and request a refund via cheque or make a credit card payment and request the refund in cash or another form.
- Payment made via virtual assets and refund is requested by other means to the customer or to a third party.

Unusual Transaction Volume or Frequency

- Numerous transactions by a customer, especially over a short period, where each transaction is not substantial, but the cumulative total is significant.
- Transactions involving virtual assets, especially where ownership cannot be easily traced to the customer.

Suspicious Online Transactions

- Indicators of suspicious online payment card-not-present transactions, such as:
 - Multiple online orders with the same shipping address but different payment cards, potentially indicating the use of stolen or fraudulent cards.
 - Same payment account but different shipping addresses, which could suggest the use of stolen payment card information shared among accomplices.
 - Same Internet Protocol (IP) address for online orders made around the same time with different payment cards, which may signify criminal activity using fraudulent payment cards.
 - Reattempting transactions with smaller amounts after an initial decline, which may indicate card testing to assess limits and available balances.

9.2.3. Supplier Behaviour

Lack of Transparency or Documentation and Forgery

- Inability to provide information for due diligence and record-keeping purposes.
- Provides forged, fraudulent, or false identity documents.
- Contracts, invoices, or other trade documents provided have vague or missing descriptions, appear counterfeit (including false or misleading information), include resubmission of previously rejected documents, or are frequently modified or amended.
- Supplier requests that normal business records not be kept.

Secrecy, Suspicious Origins and Products

- Supplier is unusually concerned with the business's Anti-Money Laundering (AML), Counter Financing of Terrorism (CFT), or Counter Proliferation Financing (CPF) policies.
- Supplier attempts to maintain a high degree of secrecy with respect to the transaction. Examples include:
 - Unwillingness to identify beneficial owners or controlling interests, where this would be commercially expected.
 - Requests for payments to be made through money services businesses or other non-bank financial institutions without apparent legitimate business purposes.
 - Vague or refusal to provide information on the reason for selling or buying PSPM or about the origin of the items.
- Supplier's origins or the material's declared country of origin appears to be fictitious.
- Entity or any of its counterparties appear to import precious metals and stones that originate from a country with limited production or no mines at all.
- Precious metals (especially gold) originating directly or indirectly from conflict-affected or high-risk areas (CAHRA), including routing through neighbouring or intermediary countries to disguise true origin.
- Repeated changes in the declared country of origin across invoices, certificates, or shipping documents.
- Reliance on unverifiable or weak origin documentation, including unsupported "mine-of-origin" claims.
- Use of private refinery letters or unverifiable assurances instead of internationally recognized responsible sourcing documentation.



- Gold sourced or transited through jurisdictions known for weak supply-chain controls, illicit gold production, or conflict financing.
- Frequent re-routing of shipments, including unnecessary transshipment hubs without economic rationale.
- Shipment of recycled or secondary gold presented as newly mined without supporting evidence.
- Rough diamonds are not accompanied by a valid Kimberley Process (KP) certificate, for example:
 - No KP certificate attached to the shipment of rough diamonds.
 - The KP certificate is forged or appears to be forged.
 - The KP certificate has an unusually long validity period.

Adverse Media or High-Risk Association

- Supplier is traced to a credible or verifiable negative news or criminal activities.
- Entity's owners, shareholders, authorized signatories, or any of its counterparties have been the subject of adverse news from a trusted media source.
- Supplier appears to be related to a high-risk country or territory, or entity associated with risks for money laundering or terrorism activities, or a person designated as a terrorist.
- Supplier transports PSPM through a country or territory designated as "high risk for money laundering or terrorism activities" without apparent economic reason.

Other Behavioural Red Flags

- Supplier appears to be in a hurry to complete the transaction or is willing to sell PSPM at a rate significantly lower than their typical sale value.
- Supplier does not appear to understand the PSPM industry or lacks the appropriate equipment or finances to engage in regulated activity in the PSPM industry.
- Supplier appears uninterested in or uninformed about the structure or transactions of their PSPM business.
- Supplier lacks operational infrastructure, staffing, or financial capacity commensurate with declared high trade volumes.

9.2.4. Supplier Transaction Behaviour

Inconsistent Transaction Profiles

- Transactions that are not consistent with the usual profile of a supplier, including:
 - Over or under-invoicing, structured or complex transactions, multiple invoice requests, or high-dollar shipments that are over or underinsured.
 - Transactions that are excessive given the amount or quality of the goods or the potential profit from the sale of PSPM.
 - Consignment size or type of PSPM shipped that appears inconsistent with the capacity of the exporter or importer (e.g., shipments or transshipments that do not make economic sense).
 - Misclassification of gold purity, weight, origin, and value on customs declaration forms.
 - The transaction involves the use of front or shell companies, which have no real operating activity. For example, the entity's ownership structure appears to be doubtful or obscure, or the entity refuses to provide additional information when requested.

Third-Party Involvement

- Transactions in which third parties are involved, either as payers or recipients of payment or PSPM, without an apparent legitimate business or economical purpose. Examples include:
 - Funds paid to a third party who is not related to the supplier, without a legitimate business purpose.
 - PSPM delivered from a third party who is not related to the supplier, without a legitimate business purpose.
- Circular movement of goods or funds between related suppliers, intermediaries, or counterparties without clear economic rationale.

Virtual Assets Transactions

- Transactions involving virtual assets, especially when the ownership of the virtual assets cannot be easily traced to the regulated dealer and supplier.



- Supplier unable to provide a clear and verifiable documents supporting the source and the origin of the virtual assets.

9.2.5. Proliferation Financing Related Red Flags

Inconsistent or Evasive Behaviour

- Vague and resistant when additional information is sought.
- Hiding relationships between legal persons using nominees and shareholders with complex structures.
- PSPM trade structures with unclear end-use, end-user, or ultimate destination of value.

Mismatched Activity

- Activity mismatches the entity line of business or end-user information mismatch with the business profile.
- Mismatch in the transaction value and the customer's financial profile.

High-Risk Geographies & Unusual Routes

- Supplier or buyer is associated with jurisdictions associated with proliferation networks, restricted technology procurement, etc.
- Transactions involving higher-risk countries or jurisdictions.
- Shipment takes a circuitous route, or transaction takes a circuitous route.
- Goods are routed via unnecessary transshipment hubs, particularly those associated with sanctions circumventions.

Inconsistencies in Information

- Inconsistencies in trade documents, financial flows, destinations, ports, addresses, etc.
- Declared value of goods not matching with the shipping documents.

9.3. Red Flag Indicators for TCSPs

9.3.1. Customer Behaviour - Individual

Reluctance or Refusal to Disclose Information

- Refuses to provide personal, business, or financial information.
- Provides insufficient, inconsistent, or suspicious information.
- Avoids personal contact or refuses in-person meetings without justification.
- Does not maintain contact after the initial establishment of a legal entity.
- Reluctant or refuses to disclose:
 - The identity of the beneficial owner.
 - Their business activities and corporate history.
 - Their source of wealth/funds.
 - The nature of their business dealings with third parties (particularly those in foreign jurisdictions).
 - Why they are conducting their activities in a certain manner.
 - Who they are transacting with.
- Customer withdraws, becomes unresponsive, or terminates the relationship following EDD requests.
- Customer applies pressure on TCSP staff to expedite incorporation or documentation while discouraging due diligence.
- Attempts to influence staff to bypass internal escalation or compliance approval processes.

Unclear Business Activities

- Has an unclear rationale for conducting activities in a specific jurisdiction.
- Is a foreign national with no significant dealings in the country and no clear economic rationale for seeking a relationship with a TCSP.
- Expresses interest in establishing or acquiring a legal entity or legal arrangement without a logical explanation or description of the purpose.
- A customer who wants to establish multiple inconsistent businesses across different emirates in the UAE, with no clear economic reasons.
- Requests to repeatedly amend company activities, licences, or constitutional documents without a commercial rationale.



Criminal or Adverse Background

- Is under investigation, has known criminal connections, or appears in adverse media linked to corruption, fraud, or financial crimes.
- Has a link to an extremist individual, a designated terrorist individual, or organization. Has been previously prohibited from holding a directorship role or operating a TCSP.
- Is listed on sanctions or watchlists.

Use of Intermediaries & Avoidance of Transparency

- Insists on using intermediaries (professional or informal) without a legitimate reason.
- Requests nominee directors or shareholders to hide ownership.
- Requests nominee directors with little experience in the required licensed business.
- A customer who is a family member or has a close association with a foreign individual or entity abroad.
- Demonstrates an excessive concern about compliance requirements or AML measures.
- Appears very concerned about or asks an unusual number of detailed questions about compliance-related matters such as customer due diligence or transaction reporting requirements.
- Requests for frequent changes to authorised signatories or powers of attorney.

Politically Exposed Persons (PEPs)

- Is a PEP or has familial/professional associations with a PEP, particularly when their involvement does not align with their official duties or declared interests.

Unusual Transaction Knowledge or Lack Thereof

- Appears unfamiliar with the details of the requested transaction.
- Shows little interest in transaction specifics, costs, or securing better terms.
- Engages intermediaries without a clear business rationale, especially if it obscures the identity of the beneficial owner.

9.3.2. Customer Behaviour - Legal Entities and Arrangements

Lack of Business Substance

- Cannot demonstrate actual business activity or provide evidence of operations.
- Has no online presence or business networking profile.
- Uses an address linked to multiple unrelated companies, indicating a mailbox service.
- Use of dormant companies that suddenly become active without a clear source of funds or business rationale.

Complex or Unnecessary Corporate Structures

- Uses overly complicated ownership or management structures without justification.
- Has frequent changes in ownership or control.
- Uses nominee agreements, shelf companies, or offshore trusts to obscure beneficial ownership.
- Requests the use of foreign private foundations that operate in secrecy jurisdictions.
- Engages in rapid changes in company ownership, management, or structure shortly after establishment without justification.
- Requests to establish companies or legal arrangements that appear designed to circumvent export controls or UN sanctions regimes.
- Use of layered corporate structures involving jurisdictions subject to UN PF-related sanctions.
- Frequent changes to ownership, directors, or business purpose shortly after sanctions designations affecting related parties.

Foreign Incorporation in High-Risk Jurisdictions

- Is registered in a tax haven or a jurisdiction with weak anti-money laundering (AML) regulations.
- Transfers incorporation or registration to another country without an apparent business reason.
- Conducts business in jurisdictions identified as high-risk for money laundering and terrorist financing.

Unusual Board or Management Practices

- Directors or shareholders are difficult to contact or do not seem actively involved.
- Uses the same individuals as directors or shareholders across multiple companies.



- Has an unusually high number of authorized signatories.
- Engages in transactions with sanctioned entities or those located in high-risk jurisdictions.
- Requests to backdate incorporation documents, share transfers, or directorship appointments.
- Requests to split ownership among multiple individuals or entities to avoid screening thresholds.
- Attempts to rapidly dissolve, redomicile, or rebrand entities following sanctions announcements.

9.3.3. Transaction Behaviour

Unexplained or Unusual Transactions

- Conducts high-value transactions that do not match their profile or financial history.
- Uses multiple accounts or sources for deposits and payments without a clear rationale.
- Requests transactions with excessive secrecy or anonymous financial instruments.
- Engages in frequent or high-value intercompany loans with no clear economic purpose.
- Sends or receives funds to/from high-risk jurisdictions without justification.
- Requests offshore accounts or companies in secrecy jurisdictions without a business reason.

Unusual Loan and Investment Behaviour

- Uses cash as collateral for loans, particularly when the funds originate from foreign institutions.
- Makes significant capital contributions inconsistent with company size or industry norms.
- Obtains financing from private third parties without proper documentation.
- Requests the use of pooled accounts or safe custody arrangements without necessity.
- Seeks to open multiple trusts or accounts with the same beneficiary.
- Seeks to open multiple trust accounts, each with a different business declared as the source of funds.
- Seeks to open trust accounts with high amounts, which are inconsistent with the customer's profile.
- Repeated establishment of trusts with the same beneficiaries across multiple jurisdictions.

Payment Methods and Funding Sources

- Uses large cash transactions or negotiable instruments that do not indicate the true payer.
- Prefers unusual payment methods (e.g., virtual assets, precious metals).
- Breaks down transactions into smaller parts to avoid reporting requirements.
- Receives payments from unrelated third parties with no apparent connection.
- Uses a TCSP's customer account for transactions without prior notification.
- Engages in excessive use of power-of-attorney arrangements without explanation.
- Requests funding from third parties without logical explanation or business justification.

Other Red Flags

- Frequently changes TCSPs without a valid reason.
- Engages multiple TCSPs for similar services without justification.
- Requests services that obscure beneficial ownership from authorities.
- Requests nominee arrangements, shelf companies, or offshore structures without a clear purpose.
- Uses legal arrangements that separate ownership and control in an unusual manner.
- Lacks transparency in operations, refusing to provide clear information about business activities.
- Uses multiple professionals or advisors in the same jurisdiction for the same transaction.
- Takes an unusual interest in assisting or helping to facilitate the business arrangements of another party.
- Provides falsified documents or counterfeit records.
- Attempts to engage in fraudulent transactions, such as multiple invoicing or over- and under-invoicing.
- Customers or beneficial owners linked to sectors associated with dual-use goods, sensitive technologies, or sanctioned trade activities.
- Customer is linked to export-controlled industries with no legitimate corporate history.
- Customer's declared business does not reflect an alignment with its financial behaviour (e.g. small consultancy claiming to import industrial machinery).



- Frequent changes in ownership, directorship, authorised signatories, particularly post sanctions updates.
- Capital injections from entities located in PF-sensitive jurisdictions.

9.4. Red Flag Indicators for IAAs

9.4.1. Customer Behaviour - Individual

Concealing or Disguising Identity of the UBO

- Use of companies, trusts, and / or bearer shares to obscure beneficial ownership.
- Use of shell companies for the placement and / or layering of the proceeds of crime.
- Use of professional intermediaries, trustees or nominee shareholders in order to provide the appearance of legitimacy and / or to obscure beneficial ownership.
- Creation or use of multi-jurisdictional structures of legal entities and legal arrangements to disguise beneficial ownership, or to facilitate a predicate offence related to ML/TF.
- The entity is owned by or affiliated with a legal entity incorporated/established in a jurisdiction that does not require companies to report beneficial owners to a central registry.
- Changing the ownership without notifying the accountant on the changes made.
- Acquires or uses shelf companies, or pre-constituted shell companies, in jurisdictions that allow their use but do not require updating of ownership information.
- When questioned about the source of funds, tax history, beneficial ownership or cross-border transactions, the individual becomes defensive, evasive or hostile.

Suspicious Behaviour or Lack of Transparency

- Customer is reluctant or refuses to provide personal information, or the accountant has reasonable doubt that the provided information is correct or sufficient.
- Refuses to co-operate or provide information, data, and documents usually required to facilitate an audit, or is unfamiliar with the details of the company's business.
- The customer is unable or refuses to explain:
 - The business activity and corporate history.
 - The identity of the beneficial owners.
 - The source of the wealth and funds.
 - The nature of their business dealings mainly with parties located in foreign jurisdictions.
 - The reason behind conducting their activities in a certain manner.
- Customer actively avoids personal contact without sufficient justification.
- Does not maintain contact or communication after initial appointment of the accountant, when this would normally be expected.
- Customer is the signatory to multiple company accounts (especially unrelated companies) without sufficient explanation.
- Makes unusual requests (including those related to secrecy) of the accountant or its employees.
- Appears very concerned about or asks detailed questions about compliance-related matters, such as customer due-diligence or transaction reporting requirements.
- Individual claims to be self-employed, operates cash-based businesses, or operates within an informal sector abroad, but fails to provide verifiable tax filings, audited financial statements, or reliable third-party verification.
- The individual is either unable or unwilling to provide tax returns from their home-country, tax residency certificates, proof of tax payments on reported income.
- There are frequent assertions of being "tax exempt" or "not required to file" without credible legal or jurisdictional justification.
- The individual requests the accountant or auditor to "simplify" explanations, accept management representations without evidence, exclude certain accounts, transactions, or jurisdictions from scope.

Unusual Customers and High-Risk or Criminal Associations

- Customer is under investigation, has known connections with criminals, has a history of criminal indictments or convictions, or is the subject of adverse information in reliable publicly available information sources.



- Customer is a politically exposed person or has familial or professional associations with a person who is politically exposed.
- Attempts to improperly conceal beneficial ownership from competent authorities.
- Has previously been prohibited from holding a directorship role in a company.
- When the entity or any of the UBO's are on any Sanctions lists or international lists.
- Funds originate from or transit through jurisdictions characterized by high tax secrecy, known for aggressive tax avoidance schemes, exhibiting weak tax enforcement or transparency.

Unusual Timing or Patterns in Transactions

- Conduct and unusual number or frequency of transactions in a relatively short time period.
- Disposes of assets under conditions which are unusual, or which involve unnecessary expense or losses, without a logical explanation.
- Makes deposits or other payments from multiple accounts or sources.

9.4.2. Customer Behaviour - Entity

- Cannot demonstrate a history or provide evidence of real activity.
- Suddenly becomes active after a long period of dormancy, without a logical explanation.
- Cannot be found on the internet, social business network platforms, or public domain.
- Is registered at an address that does not match the profile of the company, or that cannot be located on internet mapping services (such as Google Maps).
- Is registered at an address that is also listed against numerous other companies or legal arrangements, indicating the use of a mailbox service.
- Has directors or controlling shareholder(s) who cannot be located or contacted, or who do not appear to have an active role in the company, or where there is no evidence that they have authorised transactions.
- Has directors or controlling shareholder(s) and/or beneficial owner(s) who are also found to be representatives of other legal persons or arrangements, indicating the possible use of professional nominees.
- Has an unusually large number of beneficiaries and other controlling interests or has authorised numerous signatories for the transaction without sufficient explanation or business justification.
- Is not normally a cash intensive business but appears to have substantial amounts of unexplained cash.
- Provides falsified records or counterfeit documentation.
- Is owned by or affiliated with a legal entity incorporated or established in a jurisdiction with weak or absent AML/CFT laws.
- Transfers its registration or domicile from another jurisdiction without any evidence of genuine economic activity in the country of origin.
- The customer requests that shortcuts be taken, or that the work is completed in an unreasonably short time period and is prepared to pay substantially higher fees than usual in exchange.
- The customer's requested or preferred means of payment is unusual (e.g. precious metals or stones, virtual currencies, or other unconventional payment methods).
- Individuals manage multiple entities that transfer funds among themselves without corresponding commercial activity.

9.4.3. Transaction Behaviour

Concealing the Source of Funds

- Involve unexplained last-minute changes involving the identity of the parties (e.g. it is begun in one individual's name and completed in another's without a logical explanation for the name change) and/or the details of the transaction (such as the amount or terms) and/or the details of the financing or the payment instrument/procedures (e.g. a mortgage is arranged for a property purchase, but cash is substituted as the final payment method).
- Involves cash or negotiable instruments which do not state the true payer. Especially where the amount of such instruments is significant in relation to the total value of the transaction.
- Individual describes funds as originating from "family", "friends", or "community networks" without formal documentation.



Suspicious Use of Investment Schemes or Financial Instruments

- Transactions are financed by a non-financial institution third party, whether a natural or a legal person, with no logical explanation or commercial justification.
- Transactions involving loans or other financing from private third parties without adequate supporting agreements, collateral, or regular interest payments or principal repayments.
- Involve assets purchased with cash, which are then used as collateral for a loan within a short period of time.
- Involves third-party funding (either for the transaction or for fees) with no apparent connection or legitimate explanation.
- The individual injects substantial amounts into UAE entities as shareholder loans, capital contributions, advances or related-party funding lacking clear loan agreements, repayment terms, or economic justification.

Unusual Transaction Frequency or Structure

- Funds that are sent to, or received from, a foreign country when there is no apparent connection between the country and the customer, and/or which are sent to, or received from, high-risk jurisdictions.
- Involve several transactions which appear to be linked, or which involve the same parties or those persons who may have links to one another (for example, family ties, business ties, persons of the same nationality, persons sharing an address or having the same representatives or attorneys, etc.).
- A significant increase in capital, or successive capital contributions over a short period of time, for a recently incorporated company with no logical explanation.
- Personal funds are funnelled through corporate accounts, followed by personal expenditures or asset acquisitions.

Suspicious Relationships and Pressures

- Transactions involving family members of one or more of the parties without a legitimate business rationale.
- Transactions appear to involve parties with a questionable connection or generates doubts that cannot be sufficiently explained by the customer.
- Involving frequent or high-value transactions between a small number of related natural or legal persons.
- Transactions involving requests for payments to / from third parties without a substantiating reason or corresponding transaction.
- The unexplained use of powers-of-attorney or other delegation processes.
- Transactions appear to be directed by someone (other than a formal legal representative) who is not a formal party to the transaction.
- Income, occupation or business activities in an individual's home country do not align with the level of assets or capital investments observed in the UAE.
- Individual frequently utilized relatives, employees, business partners, offshore contacts to execute payments or hold assets on their behalf.
- Individual avoids appearing as the direct counterparty in transactions despite exercising actual control.

Irregularities in Contracts or Agreements

- Involving multiple appearances of the same parties in different transactions over a short period of time or involves transactions or financial transfers (e.g. disbursements or repayments) between the parties over an unusually long contractual period.
- Including contractual agreements with terms that are unusual or that do not make business sense for the parties involved.
- Unreasonable choice of accountant without a clear explanation, given the size, location or specialisation of the accountant.
- When the customer has changed the accountant a number of times in a short space of time without legitimate reason.



Transactions That Do Not Make Economic Sense

- Appointing a counterparty acting in the capacity of the director, signatory, or other authorised representative of the entity, who does not appear to have the required competency or suitability.
- There is rapid buying and selling of assets without commercial rationale (potential layering).

Other Transaction Pattern Red Flags

- Transactions executed from a business account but appears to involve personal purchases or sales, or public finances.
- Involve complicated transaction routings or multi-jurisdictional corporate structures without sufficient explanation or trade records.
- Involving foundations, cultural or leisure associations, or non-profit-making organizations, when the characteristics of the transaction do not match the goals of the entity.
- Explanations provided regarding the commercial purpose of foreign transactions are inconsistent.
- Customer claims to export technical equipment without any manufacturing capacity.
- Financial statements reflect payments to unknown suppliers in high-risk jurisdictions.
- Customer refuses to provide end-use / end-user information, customs documentation, supply chain partners.



10. Annexure I – Other Report Types

Under the UAE's AML/CFT/CPF framework, the goAML platform provides DNFBPs with the access to report suspicious activities to the FIU. Each report type serves a specific purpose and must be completed in line with the requirements and standards set by regulatory authorities. Correct categorization and timely submission are critical to ensuring the FIU can effectively examine and act on the information provided.

The following are additional report types currently available on the goAML portal as defined by the FIU:

- **Additional Information File without Transactions (AIF):** Used to provide the FIU with supplementary or additional information which is related to a previously submitted report without transaction data. Such reports are submitted when the FIU requires further details and is communicated through the "Message Board".
- **Additional Information File with Transactions (AIFT):** Similar to AIF report in terms of structure, with the exception that AIFT includes transaction details related to the case.
- **Dealers in Precious Metals and Stones Report (DPMSR)⁴:** A sector specific report for DPMS entities to declare relevant transactions and activities. A DPMS is required to file a DPMSR when:
 - ✓ Conducting a transaction with a resident or a non-resident individual for cash equal to or more than AED 55,000 or its equivalent in foreign currency.
 - ✓ Conducting transactions with companies/entities equal to or more than AED 55,000 or its equivalent in foreign currency whether in cash or through wire transfer.
- **Real Estate Activity Report (REAR)⁵:** A sector specific report for real estate brokers and agents to declare relevant transactions and activities. All real estate brokers and agents is required to file a REAR for:
 - ✓ Purchase or Sale of freehold property/real estate where the method of payment includes cash and the amount is AED 55,000 or more; be it in a single payment or multiple payments.
 - ✓ Purchase or Sale of Freehold property/real estate where the method of payment is a virtual asset for a portion or the entire property value.
 - ✓ Purchase or Sale of Freehold property/real estate where the funds used to carry out the transaction were converted from or to a virtual asset for a portion or the entire property value.
- **Confirmed Name Match Report (CNMR)⁶:** In case a Confirmed Name Match is identified on an existing customer, when screening against the UAE Local Terrorist List or the UN Consolidated List, DNFBPs must freeze without delay (within 24 hours) and prohibit making funds or other assets or services available and submit a CNMR through goAML within 5 business days of implementing the freezing measures. In case a Confirmed Name Match is identified on a potential customer (a prospective Customer) or counterparty of an existing customer in a transaction, the Reporting Entity must reject the transaction and refrain from dealing with or providing any funds or other assets or services to the Confirmed Name Match and submit a CNMR through goAML within five business days of rejecting the transaction. The report should clarify the actions taken by the Reporting Entity (rejected business relation or transaction), as well as any funds or other assets frozen in the process.
- **Partial Name Match Report (PNMR):** If a DNFBP identifies a partial match between the identifiers in the UAE Local Terrorist List or UNSC Consolidated List and a customer's information in the DNFBP's database, and the DNFBP is unable to verify the match (Confirmed Name Match or False Positive), then the result is considered a 'Partial Name Match'. In this case, the DNFBP must either suspend the transaction immediately without delay, refrain from offering any funds or other assets or services or reject the transaction

⁴ <https://www.uaefiu.gov.ae/media/vcpkgosb/reports-faqs-v1-2-29-apr-2024.pdf>

⁵ <https://www.uaefiu.gov.ae/media/sr2lwuo2/7-goaml-web-real-estate-activity-report-v1-1-20-07-2022.pdf>

⁶ Previously known as Funds Freeze Report (FFR); Refer to TFS Guideline issued by EOCN



and submit a PNMR through the goAML platform within 5 business days from rejecting the transaction or any suspension measure taken.

- **Request for Information without Transactions (RFI):** When the FIU require further information from multiple reporting entities rather than just the entity responsible for submitting the STR/SAR, then an RFI request will be sent out to the concerned reporting entities through the GoAML Message Board. In such cases, the reporting entities are required to submit an RFI report through the platform.
- **Request for Information with Transactions (RFIT):** When the FIU require further information that includes transactions from multiple reporting entities rather than just the entity responsible for submitting the STR/SAR, then an RFIT request will be sent out to the concerned reporting entities through the GoAML Message Board. In such cases, the reporting entities are required to submit an RFI report through the platform.
- **High Risk Country Transaction Report (HRC):** If, during the establishment or course of the customer relationship, or when conducting transactions on behalf of a customer or a potential customer, a reporting entity identifies transactions related to high-risk countries as defined by the National Anti-Money Laundering and Combating the Financing of Terrorism and financing of Illegal Organizations Committee. In such instances, the reporting entity should file an HRC report to the FIU. The reported transactions may only be executed three working days post the reporting to the FIU, and if the FIU does not object going through with the transactions within the set period.

A comprehensive list of High-Risk Countries can be found on NAMLCFTC website at the following link <https://www.namlcftc.gov.ae/en/more/jurisdictions/>

- **High-Risk Country Activity Report (HRCA):** If, during the establishment or course of the customer relationship, or when conducting an activity on behalf of a customer or a potential customer, a reporting entity identifies activities related to high-risk countries as defined by the National Anti-Money Laundering and Combating the Financing of Terrorism and financing of Illegal Organizations Committee. In such instances, the reporting entity should file an HRCA report to the FIU. The reported activities may only be executed three working days post the reporting to the FIU, and if the FIU does not object going through with the activities within the set period.

A comprehensive list of High-Risk Countries can be found on NAMLCFTC website at the following link <https://www.namlcftc.gov.ae/en/more/jurisdictions/>