GUIDANCE NOTE

REPORTING OBLIGATIONS FOR DEALERS IN PRECIOUS METALS AND STONES ON SUSPICIONS OF MONEY LAUNDERING OR TERRORIST FINANCING

1 INTRODUCTION

1.1 It is important to protect Kuwait against both money laundering, terrorist financing, and proliferation financing, because such types of crime can undermine the economic stability and security of the country, given that these crimes are supportive of organised crime and terrorism, and they weaken the integrity of the Kuwaiti financial system and other important businesses and professions. Dealers in Precious Metals and Stones (DPMS) play an important role in protecting Kuwait against these kinds of crimes.

1.2 **Dealers in Precious Metals and Stones (DPMS) covered by the legislation on money laundering and terrorist financing**

1.3 Article 1 of law no. 106 of 2013 on Anti-Money Laundering and Combatting the Financing of Terrorism sets out that "Sole-proprietors and commercial companies dealing in gold, precious stones and precious metals when engaging in any cash transaction as determined by the Executive Regulation of this Law" are covered by the law. In the following points these professions are referred to as "dealers in precious metals and stones" or "DPMS".

1.4 **What is money laundering?**

1.5 Money laundering is the process of disguising the origins of illegally obtained money to make it appear as though it comes from legitimate sources. Money laundering is thus always associated with an under-lying proceed-generating crime, the so-called predicate crime. Money laundering schemes can be very simple or highly sophisticated. Examples of simple money laundering operations are breaking up large amounts of cash into smaller sums and depositing into a bank account, transporting cash across borders, or buying high value goods such as artworks or precious metals and stones.

A more sophisticated money laundering operation might involve a complex layer of financial transactions, such as converting cash into monetary instruments or using offshore shell companies to disguise the origin of the proceeds.

1.6 What is terrorist financing?

1.7 Terrorist financing is the process of directly or indirectly raising/collecting, moving, or using funds to support terrorist activities, individual terrorists, or terrorist organizations. These funds can be used for various purposes, including planning attacks, recruiting members, spreading propaganda, acquiring weapons, and establishing networks or safe havens. The funds or assets used for terrorism can come from both legal and illegal sources, making it challenging to detect.

1.8 What are the main differences between money laundering and terrorist financing?

1.9 The Customer Due Diligence (CDD) requirements that so-called obliged entities, including dealers in precious metals and stones, will have to comply with, are very much the same for money laundering and terrorist financing, since the financial system and other relevant businesses and professions (such as DPMS) can be misused by both money launderers and terrorist financiers. However, conceptually there are differences between the two types of serious crimes, some of which are shown in the table right below:

	Money Laundering	**Terrorist Financing**
Motivation	Financial gain and/or financing of new crimes.	Funding of terrorist activities, for example for political or ideological reasons.
Source of funds	Always an underlying predicate crime to generate the proceeds.	The funding can be through both legal and illegal sources.
Amounts involved	Often involves large sums of money.	Generally, smaller amounts are needed for the terrorist activities, so transactions are often smaller and thereby hard to detect.
Methods of concealment	Both simple and complex money laundering schemes exist, but professional money launderers often use complex transactions, shell companies, offshore accounts, and investments to make funds appear legitimate.	Often uses simpler and harder-to-detect methods, like small wire transfers, cash smuggling, crowdfunding, or "front" organizations such as charities.

2 MONEY LAUNDERING AND TERRORIST FINANCING RISKS ASSOCIATED WITH PRECIOUS METALS AND STONES

2.1 The Financial Action Task Force (the FATF) is the most important global standard setter in relation to anti-money laundering and combatting the financing of terrorism. The FATF has issued different policy documents in relation to the money laundering and terrorist financing risk related to DPMS, including a July 2015 report on "Money laundering / terrorist financing risks and vulnerabilities associated with gold". This report provides a series of case studies and red flag indicators to raise awareness of the key vulnerabilities of gold and the gold market.

2.2 The money laundering and terrorist financing risks of the precious metals and stones market are also addressed in the June 2022 money laundering and terrorist financing National Risk Assessment of Kuwait and in the AML/CFT Mutual Evaluation Report (MER) of Kuwait adopted October 2024 by the FATF.

2.3 The June 2022 National Risk Assessment of Kuwait

Kuwait in June 2022 adopted a National Risk Assessment (NRA) on money laundering and terrorist financing, which also addresses dealers in precious metals and stones. It is noted that gold, precious metals, and gemstones are very popular in the State of Kuwait. Since the ancient history of Kuwait, there is still a great demand by many people to acquire them for the purpose of adornment and other purposes. The trade in gold, precious metals, and gemstones is considered one of the most important types of trade in the State of Kuwait. Because of its high value, it constitutes a safe haven for savings and investment. The gold and precious metals sector is considered one of the sectors that attract money laundering in its three stages (deposit/replacement, camouflage, and merger), which money launderers can exploit to carry out their illegal activities in order to achieve their goal, due to the high value, light weight and small size (gemstones), ease of transportation and frequent circulation, as it is easy to sell gemstones, precious metals and gold jewelry in the State of Kuwait. At the time of the NRA there were 2,361 companies in the precious metals and stones industry being supervised by the AML/CFT Department of the Ministry of Commerce and Industry (MOCI).

2.4 As for the specific risk associated with the precious metals and stones sector the NRA states the following:

"The level of money laundering risks to which the gold, precious metals and gemstones sector is exposed in the State of Kuwait is Medium (M). The level of risk is a result of the level of threat to which the sector is exposed is Medium Low (ML) and sector vulnerabilities assessed as Medium High (MH)"

"The threat level facing the gold, precious metals and gemstones sector, which is assessed as Medium Low (ML), arises from: There are (4) investigations and trials in money laundering cases involving this sector and (2) convictions. The sector's vulnerabilities, which were assessed at a medium-high level (MH), result from: Lack of human resources and electronic systems in place for the employees of the supervisory authority during the period subject to evaluation, lack of enforcement of some administrative and criminal penalties, failure of compliance controllers to fully perform their role, lack of reporting of suspicious transactions, and lack of sufficient information related to knowing the real beneficiary. It was found that among the risks that this sector is exposed to is the small size of the product, and the ease of its handling and transporting it between countries. The process of assessing money laundering and terrorist financing risks at the national level took into account the type of products."

2.5 The October 2024 Mutual Evaluation Report (MER) of Kuwait

2.6 The MER does in fact not write very much about the dealers in precious metals and stones. It is stated that MOCI is not going to issue a business license if a dealer has been convicted of certain crimes, but the list of crimes is not very long or comprehensive. There is no information about any Suspicious Transaction Reports (STRs) being submitted by DPMS.

2.7 Why Criminals Use Precious Metals and Stones?

Precious metals and stones are attractive to money launderers and terrorist financiers because they combine high value, portability, liquidity, and relative anonymity. Gold, diamonds, gemstones, and other precious commodities can store substantial value in a compact and easily transportable form, allowing criminals to easily move and conceal illicit assets.

These commodities may also be used as alternative value transfer mechanisms outside the formal financial system. In some cases, individuals may convert illicit cash into gold or other precious assets and later sell or transport them across borders, making it more difficult to trace the origin and movement of funds.

The sector may also be vulnerable to trade-based money laundering, where commodities are over- or under-invoiced, repeatedly traded, or moved across jurisdictions using complex arrangements. These characteristics make the DPMS sector particularly exposed to misuse for money laundering, terrorist financing, and sanctions evasion.

Understanding why criminals are attracted to the DPMS sector can help dealers in Precious Metals and Stones (DPMS) recognize suspicious behaviour and better understand the rationale behind many of the red flags described later in this Guidance Note.

2.8 Common DPMS Money Laundering Typologies

Dealers in precious metals and stones should be aware of common typologies used to exploit the sector. These include:

- conversion of illicit cash into gold, jewelry, or gemstones;
- segmenting or structuring transactions to avoid reporting thresholds or internal controls;
- use of third parties, nominees, or shell companies to conceal the true purchaser or beneficial owner;
- repeated buying and selling of the same commodities to obscure the origin of funds;
- cross-border movement of precious metals or stones in order to transfer value;
- trade-based money laundering involving false invoicing or misrepresentation of value;
- use of precious metals or stones as an alternative to the banking system;
- use of the sector to facilitate sanctions evasion;
- involvement of complex or unusual commercial arrangements without clear economic rationale.

Understanding these patterns supports more effective detection of suspicious activity.

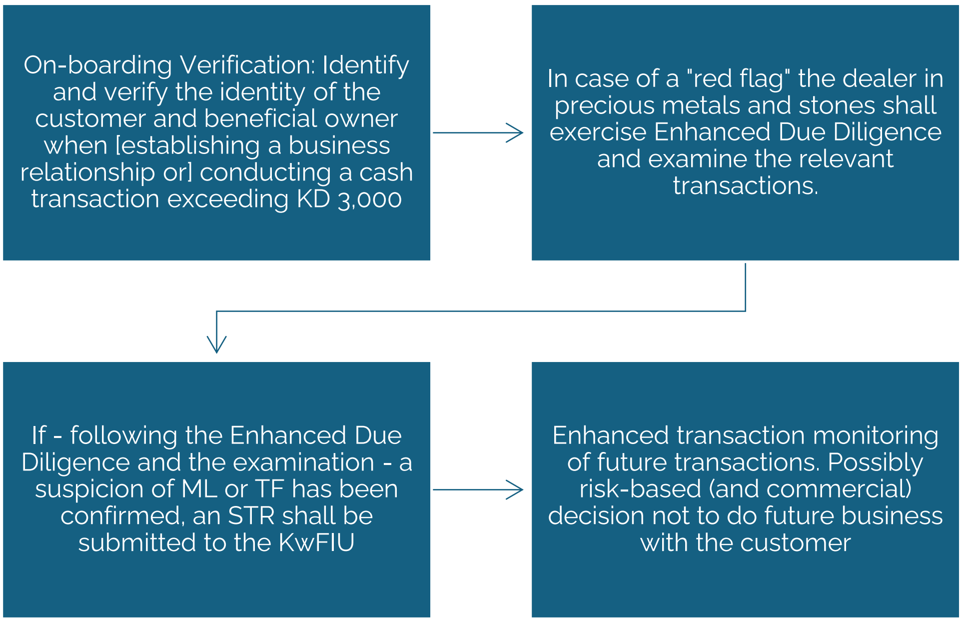
3 HIGH-LEVEL CUSTOMER DUE DILIGENCE (CDD) REQUIREMENTS FOR DEALERS IN PRECIOUS METALS OR STONES OF RELEVANCE TO REPORTING

3.1 Relevant legal basis

3.2 International organizations such as the FATF have defined standards on how countries are supposed to fight money laundering and terrorist financing. There are several different provisions, many of them of relevance to the reporting obligation. Kuwait have implemented these standards into national policies, co-operation practices between the relevant authorities, and legislation. In Kuwait the most important single piece of legislation is law no. 106 of 2013. This law is supported by Ministerial Resolution no. 37 of 2013 - Executive Regulation for Law 106 of 2013.

3.3 DPMS High-level CDD requirements of direct relevance to reporting

3.4 The high-level Customer Due Diligence (CDD) requirements for dealers in precious metals and stones of direct relevance to the reporting obligation can be illustrated by the following process diagram:



3.5 According to Article 1 of Law No. 106 of 2013, a "business relationship" is expected to have an element of duration. In reality, such an element of duration is probably rarely seen in the precious metals and stones sector that for the most consists of single transaction. Furthermore, Article 1 refers specifically to "transactions" when defining dealers in precious metals and stones as a "designated non-financial business and profession" i.e., a non-financial business/profession comprised by Law No. 106 of 2013 (which is why the words "establishing a business relationship or" is in square brackets in the first box above).

3.6 The threshold of KD 3,000 is defined in the Ministerial Resolution no. 37 of 2013. That the CDD requirements (and thereby also reporting obligations) apply for dealers in precious metals and stones only for cash transactions follows directly from Article 1 of Law No. 106 of 2013.

3.7 Ministerial Resolution no. 182 of 2025 strictly prohibits cash payments in all sale or purchase transactions of gold, precious stones and precious metals.

3.8 "Red flags" specifically for dealers in precious metals and stones will be detailed further below under Section 5 of this Guidance Note, and the reporting obligation, including the concepts of an STR and the FIU, will be detailed further under Section 5.

3.9 Article 16 of the Ministerial Resolution defines a time limit of 2 days for reporting to the KwFIU after a suspicion (or reasonable grounds to suspect) has materialised.

3.10 Relationship Between Customer Due Diligence and Suspicious Transaction Reporting

CDD is a fundamental component of an effective anti-money laundering and counter-terrorist financing framework and provides the basis for the identification and reporting of suspicious transactions. Effective suspicious transaction reporting depends on a reporting entity's ability to understand who its customers are, who ultimately owns or controls them, the nature and purpose of the transaction, and whether the transaction is consistent with the customer's known profile and financial circumstances.

Customer identification enables dealers in precious metals and stones to establish and verify the identity of the parties involved in a transaction and helps ensure that suspicious activity can be linked to specific individuals or entities. Accurate and complete customer information also supports the quality and usefulness of STRs by providing the KwFIU with reliable information that can be analysed and, where appropriate, disseminated to competent authorities.

Obtaining and verifying beneficial ownership information is equally important. Criminals frequently seek to conceal their involvement in DPMS sector transactions using nominees, intermediaries, family members, legal entities, or other arrangements intended to disguise the identity of the true owner. Understanding who ultimately owns or controls the customer or benefits from the transaction is therefore essential to identifying suspicious activity and ensuring that STRs provide meaningful financial intelligence.

Information regarding the source of funds and source of wealth also plays a critical role in the assessment of suspicious activity. dealers in Precious Metals and Stones (DPMS) should seek to understand whether the funds used in a transaction are consistent with the customer's known profile, occupation, business activities, and financial circumstances. Where the source of funds or source of wealth cannot be adequately explained, or appears inconsistent with the transaction, this may constitute an indicator of money laundering or terrorist financing and should be subjected to further scrutiny.

Customer due diligence information establishes the baseline against which unusual or suspicious activity is assessed. Suspicion often arises because a transaction or customer behaviour is inconsistent with the information obtained during the CDD process. Accordingly, effective customer due diligence supports the identification of suspicious activity and contributes directly to the quality and effectiveness of suspicious transaction reporting.

Conversely, weak or incomplete customer due diligence can significantly impair the quality of STRs. Inadequate customer identification, incomplete beneficial ownership information, or insufficient understanding of the customer's source of funds and source of wealth may prevent reporting entities from identifying suspicious activity or providing the KwFIU with sufficient information to conduct effective analysis

3.11 Enhanced Due Diligence and Suspicion Assessment

Enhanced Due Diligence (EDD) is intended to provide reporting entities with a deeper understanding of higher-risk customers, transactions, and business relationships. The purpose of EDD is not simply to collect additional documents, but to enable reporting entities to better understand the source of wealth, source of funds, ownership arrangements, and economic rationale underlying a transaction, thereby supporting more effective risk management and suspicious activity detection.

EDD measures should be applied where higher risks are identified, including situations involving politically exposed persons, complex ownership structures, high-risk jurisdictions, unusual transaction patterns, or other circumstances presenting elevated money laundering or terrorist financing risks.

Depending on the circumstances, enhanced due diligence may involve obtaining additional information regarding the customer's business activities, source of wealth, source of funds, beneficial ownership, intended use of the transaction, or the purpose and nature of the transaction. Reporting entities may also seek information concerning counterparties, intermediaries, financing arrangements, or other parties involved in the transaction.

EDD may require the collection and review of additional supporting documentation. Such documentation may include information evidencing the source of wealth or source of funds, bank statements, corporate documents, financial statements, tax records, sales contracts, financing agreements, or other records relevant to understanding the transaction and assessing its legitimacy.

The purpose of enhanced due diligence is to enable reporting entities to determine whether concerns identified during the customer due diligence process or transaction monitoring can be reasonably explained. In some cases, additional information obtained through enhanced due diligence may resolve concerns and confirm that the transaction is consistent with the customer's profile and legitimate business activities. In other cases, enhanced due diligence may reveal inconsistencies, unexplained wealth, concealed ownership arrangements, or other indicators that strengthen suspicion.

Accordingly, enhanced due diligence should be viewed as an important tool supporting suspicious transaction reporting. The information obtained through enhanced due diligence assists reporting entities in determining whether there are reasonable grounds to suspect that a transaction or attempted transaction may involve money laundering, terrorist financing, or related criminal conduct and whether an STR should be submitted to the KwFIU.

4 STR REPORTING AS AN END-TO-END PROCESS

Suspicious Transaction Reporting should not be viewed as an isolated compliance obligation triggered solely by the identification of one or more red flags. Rather, effective suspicious transaction reporting is the result of a series of interconnected AML/CFT controls that allow dealers in Precious Metals and Stones (DPMS) to understand their customers, monitor transactions, identify unusual activity, and assess whether there are reasonable grounds to suspect money laundering or terrorist financing.

The purpose of these controls is not simply to satisfy regulatory requirements, but to enable reporting entities to detect suspicious activity and provide the KwFIU with meaningful financial intelligence that can support investigations and the protection of the financial system.

4.1 STR Reporting as the Outcome of AML/CFT Controls

The identification and reporting of suspicious transactions are the outcome of a broader risk-based process. Suspicion rarely arises from a single event and is usually formed through the combination of several controls and sources of information.

Customer due diligence measures provide the information necessary to understand who the customer is, who ultimately owns or controls the transaction, and what the expected purpose and nature of the transaction are. Customer risk assessments help identify customers, beneficial owners, transactions, or circumstances that may require greater scrutiny.

Transaction monitoring and ongoing interaction with customers enable dealers in Precious Metals and Stones (DPMS) to identify activity that appears unusual, inconsistent, or lacking an apparent economic rationale. Where concerns arise, those concerns should be escalated internally and subjected to further review and examination. Depending on the size and structure of the reporting entity, this review may be conducted by compliance personnel, management, or other designated individuals responsible for AML/CFT matters.

The internal examination process should seek to determine whether the unusual activity can be reasonably explained or whether there are reasonable grounds to suspect that the transaction or attempted transaction may involve money laundering, terrorist financing, or related criminal conduct. Where such grounds exist, an STR should be submitted to the KwFIU without delay.

Accordingly, suspicious transaction reporting should be viewed as the culmination of a process involving customer due diligence, customer risk assessment, transaction monitoring, internal escalation, internal investigation, and management or compliance review, rather than as a stand-alone event.

4.2 Relationship Between Customer Understanding and Suspicion

Suspicion is often formed because a transaction, customer behaviour, or ownership arrangement is inconsistent with what would normally be expected based on the information known about the customer.

Understanding the customer is therefore fundamental to the identification of suspicious activity. dealers in Precious Metals and Stones (DPMS) are expected to obtain sufficient information regarding the customer's identity, beneficial ownership, source of funds, source of wealth, occupation or business activity, and the purpose of the transaction. This information establishes a baseline against which unusual or unexpected activity can be assessed.

Suspicion may arise where the value of the transaction appears inconsistent with the customer's known financial profile or business activities. Similarly, concerns may arise where the source of wealth or source of funds used to finance the transaction cannot be reasonably explained or appear inconsistent with the customer's declared circumstances.

Suspicion may also arise where a transaction lacks an apparent economic or lawful purpose. Examples include situations where the customer demonstrates little interest in the characteristics or value of gold, purchases or sells gold in a manner that does not appear commercially rational or uses unnecessarily complex structures or intermediaries without a clear explanation.

The presence of one or more red flags does not automatically mean that money laundering or terrorist financing is occurring. However, when unusual activity cannot be adequately explained, or when multiple indicators are present, the transaction should be subjected to further examination and, where appropriate, reported to the KwFIU.

The unique characteristics of the Dealers in Precious Metals and Stones (DPMS) sector make customer understanding particularly important for the identification and assessment of suspicious activity. Unlike many other types of transactions, purchases and sales involving precious metals and stones frequently involve highly portable stores of value, significant cash transactions, rapid conversion between different forms of value, and cross-border movement of commodities. These characteristics make the sector particularly attractive to criminals seeking to conceal, preserve, transfer, or integrate illicit proceeds.

Accordingly, understanding the customer's profile, business activities, source of funds, source of wealth, and the economic rationale underlying a transaction is essential to determining whether unusual activity may be indicative of money laundering or terrorist financing.

Suspicion may arise where the customer's profile, financial circumstances, or known business activities appear inconsistent with the nature or value of the transaction. Similarly, concerns may arise where customers are unable or unwilling to explain the source of significant funds, seek to purchase high-value commodities without an apparent commercial or investment rationale, or engage in transactions that appear inconsistent with their known profile or expected behavior.

In the DPMS sector, the conversion of cash into gold, precious stones, jewelry, or other highly liquid assets may provide criminals with an effective means of storing or transferring value. Accordingly, customers who demonstrate unusual urgency, conduct repeated high-value purchases, show little interest in the quality, characteristics, or price of the commodities involved, or appear focused primarily on converting one form of value into another may warrant additional scrutiny.

Similarly, suspicion may arise where transactions involve unusual payment arrangements, unexplained third-party funding, multiple purchases conducted in close succession, or structures that appear unnecessarily complex or lack an apparent economic purpose. Customers who seek to divide purchases into multiple transactions, repeatedly convert commodities into different forms, or utilize intermediaries or legal entities without a clear explanation may also present elevated risks.

The international nature of the precious metals and stones trade further reinforces the importance of customer understanding. Transactions involving cross-border movement of commodities, foreign counterparties, or jurisdictions unrelated to the customer's profile or business activities may increase risk and should be assessed in light of the customer's known circumstances and the overall purpose of the transaction.

The presence of any of these characteristics does not automatically mean that money laundering or terrorist financing is occurring. However, where customer behavior, transaction characteristics, source of funds, ownership arrangements, or the apparent purpose of the transaction cannot be reasonably explained, reporting entities should consider whether there are reasonable grounds to suspect that the activity may involve criminal conduct and whether further examination, internal escalation, or the submission of a Suspicious Transaction Report to KwFIU is warranted.

Reporting entities should therefore adopt a risk-based and contextual approach to suspicious activity detection and should avoid relying exclusively on lists of red flags or isolated indicators. Suspicion should be formed through an assessment of all relevant facts and circumstances known to the reporting entity at the time.

4.3 Integration into Daily Business Operations

The identification of suspicious activity is not solely the responsibility of compliance personnel or senior management. In practice, the earliest indicators of suspicious activity are often identified by individuals who interact directly with customers and transactions on a daily basis.

Dealers in Precious Metals and Stones (DPMS), sales personnel, administrative staff, and other customer-facing employees are often in the best position to observe unusual customer behaviour, inconsistencies in explanations, reluctance to provide information, unusual payment arrangements, or other indicators that may suggest money laundering or terrorist financing risks.

Employees involved in customer interactions should therefore remain vigilant and understand the importance of promptly escalating concerns in accordance with internal procedures. Effective suspicious transaction reporting depends upon cooperation between operational staff and those responsible for AML/CFT compliance and oversight.

Reporting entities should foster a culture in which employees understand that identifying and escalating suspicious activity forms part of their professional responsibilities and contributes to protecting the integrity of the DPMS sector and the financial system of Kuwait.

Suspicious transaction reporting should therefore be regarded as an integral part of day-to-day business operations and a shared responsibility across the organization rather than a task performed exclusively by compliance personnel.

4.4 Understanding Suspicion in the DPMS Context

In the DPMS sector, suspicion often arises not from a single indicator, but from the interaction of several factors that, when viewed together, suggest that a transaction or customer activity may involve money laundering or terrorist financing.

Such factors may include unusual customer behaviour, atypical transaction structures, the use of cash or other unusual payment methods, concerns regarding the source of funds or source of wealth, difficulties identifying beneficial owners, unusual business arrangements, or the involvement of higher-risk jurisdictions. Individually, these factors may have legitimate explanations. However, when several indicators are present simultaneously, or when they are inconsistent with the customer's known profile and the apparent purpose of the transaction, they may give rise to suspicion.

Reporting entities should therefore assess transactions and customer activity in their entirety and consider the broader context in which they occur. Suspicious activity frequently becomes apparent only when multiple indicators are viewed together rather than in isolation.

4.5 The Role of Professional Judgment

Red flags, common patterns, internal procedures, and reporting thresholds are important tools for identifying suspicious activity. However, they cannot replace professional judgment.

The determination of whether a transaction or attempted transaction is suspicious ultimately requires reporting entities to assess all the facts and circumstances available at the time. Not every suspicious situation will correspond to a predefined red flag, and not every red flag will necessarily result in suspicion.

Accordingly, reporting entities should consider the totality of the information available, including the customer's profile, the purpose and structure of the transaction, source of funds, ownership arrangements, and any other relevant circumstances. Suspicious transaction reporting should be based on a risk-based assessment and the exercise of sound professional judgment, rather than on the mechanical application of checklists or rigid thresholds.

5 RED FLAGS FOR MONEY LAUNDERING OR TERRORIST FINANCING IN DPMS SECTOR

5.1 What Is a Red Flag?

Red flags are indicators or warning signs that may suggest that a transaction or customer activity involves money laundering, terrorist financing, or other criminal conduct. Red flags are intended to assist reporting entities in identifying unusual activity that may warrant additional scrutiny and should be viewed as an important tool within a risk-based approach to anti-money laundering and counter-terrorist financing.

The presence of a red flag does not, by itself, constitute proof that a transaction is suspicious or that criminal activity has occurred. Similarly, the existence of a single red flag does not automatically require the submission of an STR. Rather, red flags should be considered indicators that may justify further examination.

The significance of a red flag depends on the surrounding circumstances and the information available to the reporting entity. In some situations, a reasonable explanation may exist for activity that initially appears unusual. In other cases, the presence of several red flags, particularly when considered together, may increase concern and strengthen the basis for suspicion.

Accordingly, red flags should not be assessed in isolation. DPMS should consider the overall context of the transaction and apply professional judgment when determining whether additional inquiries, internal escalation, or reporting are necessary.

5.2 How Red Flags Should Be Assessed?

When a red flag is identified, reporting entities should consider the nature and significance of the indicator in light of the information available regarding the customer and the transaction. Some indicators may have a reasonable explanation, while others may justify additional examination or internal escalation.

The significance of a red flag may depend on whether it occurs in isolation or together with other indicators. Although a single indicator may be sufficient to raise concerns in certain circumstances, the presence of multiple indicators generally increases the level of risk and may strengthen the basis for suspicion.

DPMS should assess red flags in the context of the customer's profile, occupation, business activities, financial circumstances, source of wealth, and source of funds. Consideration should also be given to the purpose of the transaction, the characteristics of the transaction, the parties involved, financing arrangements, and any unusual or unexplained aspects of the transaction.

Where concerns cannot be reasonably resolved, they should be escalated in accordance with the reporting entity's internal policies and procedures. Reporting entities should maintain appropriate records of the information reviewed, the analysis performed, and the basis for any decisions taken.

5.3 Red Flags and the Formation of Suspicion

The existence of a red flag does not automatically mean that an STR should be submitted. Suspicion does not arise solely because one or more indicators are present, but rather through the assessment and analysis of all the facts and circumstances known to the reporting entity.

Suspicion is formed when, after considering the available information, there are reasonable grounds to believe that a transaction or attempted transaction may involve money laundering, terrorist financing, or related criminal conduct. Reporting entities are not required to prove that criminal activity has occurred, nor are they expected to establish certainty before submitting an STR.

The decision to file an STR should therefore be based on professional judgment and an assessment of the customer, the transaction, the source of funds, ownership arrangements, and any unusual or unexplained circumstances. Red flags serve as indicators that support this assessment process and should be considered together with all other relevant information available to the reporting entity.

The presence of one or more of these indicators does not necessarily mean that money laundering or terrorist financing is taking place. However, where such indicators are identified, reporting entities should consider whether further examination, internal escalation, or the submission of an STR to the KwFIU may be appropriate.

5.4 Sector-Specific Red Flag Indicators

Please refer to the Annex for sector-specific red flag indicators.

6 EXAMINATION AND REPORTING OF SUSPICIOUS TRANSACTIONS

6.1 Internal Escalation, Investigation, and Decision-Making

The identification and reporting of suspicious transactions require effective internal processes that enable concerns to be promptly identified, escalated, examined, and, where appropriate, reported to the KwFIU.

Suspicious transaction reporting should not be viewed as a mechanical process triggered solely by the presence of one or more red flags, but rather as the result of a structured process involving the assessment and analysis of all relevant facts and circumstances.

6.2 Role of Frontline Personnel

Dealers in Precious Metals and Stones (DPMS), sales personnel, and other customer-facing employees are often the first individuals to identify unusual activity or suspicious behavior. Through their direct interaction with customers and transactions, they may observe inconsistencies, unusual urgency, reluctance to provide information, unexplained involvement of third parties, or other indicators that warrant additional scrutiny.

Employees involved in customer interactions should remain vigilant and promptly escalate concerns in accordance with the reporting entity's internal policies and procedures. The early identification and escalation of unusual activity are essential to the effectiveness of the reporting process.

6.3 Role of Compliance Personnel

Compliance personnel play an important role in reviewing information received through internal escalation channels and conducting additional analysis where necessary. This may include obtaining additional information, reviewing customer records, assessing the significance of identified red flags, and determining whether there are reasonable grounds to suspect that a transaction or attempted transaction may involve money laundering or terrorist financing.

The role of compliance personnel is not to establish that criminal conduct has occurred, but rather to determine whether sufficient grounds exist to warrant reporting to the KwFIU.

6.4 Role of Senior Management

Senior management should ensure that appropriate policies, procedures, and internal controls are in place to support effective suspicious transaction reporting. Senior management should foster a culture of compliance, ensure that employees understand their responsibilities, and provide adequate resources to support the identification, escalation, and reporting of suspicious activity.

Suspicious transaction reporting should be viewed as a shared responsibility across the organization and not solely as the responsibility of compliance personnel.

6.5 Internal Documentation

Reporting entities should maintain adequate records of internal escalations, information reviewed, inquiries conducted, and decisions made regarding suspicious activity. Such documentation supports the quality of STRs and demonstrates that appropriate consideration was given to unusual transactions and customer behavior.

Internal records should include, where appropriate, the information reviewed, additional inquiries performed, the rationale supporting the decision reached, and any action taken by the reporting entity.

6.6 Examination of Suspicious Activity

As mentioned under Section 3, it follows from Article 5 of Law No. 106 of 2013, that a transaction needs to be further examined if it is complex and unusually large or if there is a pattern of transactions for which there are no clear economic or visible lawful purpose or objective. The red flags are used to determine whether such an examination is needed.

An examination according to Article 5 is usually conducted by the risk function of the business entity or the compliance function, i.e., operational staff with insights into money laundering and terrorist financing risks. If this function assesses the transaction to be suspicious this assessment is usually escalated up the formal hierarchy with the dealers in Precious Metals and Stones (DPMS) and the formal decision to submit a report to KwFIU is usually taken by persons higher up the formal hierarchy. In some reporting entities, there is a designated committee established for this purpose, however, due to their usual size, this is probably not the case with dealers in Precious Metals and Stones (DPMS), where the decision normally would be taken by the Director or owner.

The legislation does not define a maximum timeline for the examination, just like there is no timeline defined for the escalation and formal decision-making by the hierarchy of the company. However, these processes obviously need to be concluded as quickly as possible.

6.7 Suspicious Transaction Reporting

When the dealers in Precious Metals and Stones (DPMS) have taken the formal decision that a transaction shall be deemed suspicious, an STR shall be sent to the KwFIU. Suspicious transactions or attempted transactions should be reported “without delay”.

6.8 When Does Suspicion Arise?

Suspicion arises when, after considering the available information, there are reasonable grounds to suspect that a transaction or attempted transaction may involve money laundering, terrorist financing, or related criminal conduct.

Reporting entities are not required to establish certainty or prove that criminal activity has occurred before submitting a STR. The reporting obligation is based on suspicion rather than proof.

Reasonable grounds to suspect may arise from the presence of one or more red flags, unusual customer behavior, inconsistencies between the transaction and the customer's profile, unexplained sources of funds, complex ownership structures, or other circumstances that lack an apparent economic or lawful purpose.

The determination that a transaction is suspicious should result from an assessment of all relevant facts and circumstances. Reporting entities should apply professional judgment and consider whether the activity can be reasonably explained. Where concerns remain after appropriate review, an STR should be submitted to the KwFIU.

The term "without delay" gives very little time available, and in any case the STR needs to be submitted to KwFIU no later than 2 working days after the suspicion (or reasonable grounds to suspect) has materialised as per Article 16 of the Ministerial Resolution no. 37 of 2013.

Reporting entities are required to submit STRs within the timeframes established by applicable laws and regulations. However, suspicious activity should be escalated, reviewed, and reported as soon as practicable once suspicion has been formed.

The statutory deadline represents the maximum period permitted for reporting and should not be interpreted as a target for submission. Reporting entities are expected to ensure that concerns identified by employees are promptly escalated and reviewed without unjustifiable delay.

Reporting entities should not postpone reporting solely for the purpose of obtaining additional information or attempting to establish certainty. The obligation to report arises once there are reasonable grounds to suspect that a transaction or attempted transaction may involve money laundering or terrorist financing.

Prompt reporting enhances the ability of the KwFIU and competent authorities to analyze suspicious activity and, where appropriate, take timely action

It follows explicitly from both Article 12 of Law No. 106 of 2013 and Article 15 of Ministerial Resolution no. 37 of 2013, that a suspicion has to be reported "regardless of its value". In that context the threshold of KD 3,000 that follows from Article 6 of the Ministerial Resolution should be born in mind, meaning that in reality an STR might be required even where the dealers in Precious Metals and Stones (DPMS) have not (yet) exercised CDD against the customer.

6.9 Attempted Transactions

The obligation to report suspicious activity applies not only to completed transactions but also to attempted transactions and other situations where suspicious activity is identified, even if the transaction is not ultimately completed.

Attempted transactions may include situations in which customers abandon or cancel transactions, refuse to proceed with a transaction, or terminate discussions after being requested to provide customer due diligence information or documentation. Suspicion may also arise where customers withdraw from the transaction after questions are raised regarding the source of funds, beneficial ownership, or the purpose of the transaction.

The fact that a transaction was not completed does not eliminate the possibility that money laundering or terrorist financing may have been involved. In some cases, customers may intentionally abandon transactions to avoid scrutiny or compliance measures.

Accordingly, reporting entities should consider whether aborted transactions, refused transactions, or situations in which customers unexpectedly discontinue the transaction give rise to reasonable grounds to suspect money laundering or terrorist financing. Where such grounds exist, an STR should be submitted to the KwFIU, even if the transaction was never completed.

6.10 Nature and content of an STR

An STR is not a police complaint or a police report, and the STR cannot be used by law enforcement or prosecution as evidence of criminality. An STR is a piece of intelligence that the KwFIU can utilise in its work.

An STR shall usually include the following:

1. The information of the customer in question, i.e., name, address, ID, occupation etc.
2. The transaction in question, i.e., amount, currency, date, method, involved parties, purpose etc.
3. All information related to the examination leading to the reporting, including analysis
4. The reason for suspicion, i.e., explanation of the "red flags" (this part of the STR is called the narrative).
5. Supporting documentation (if applicable), e.g. transaction records, copies of CDD documents etc.

6.11 STR Quality Expectations

The usefulness and effectiveness of an STR depend not only on whether it is submitted, but also on the quality of the information it contains. High-quality STRs provide the KwFIU with meaningful financial intelligence that facilitates analysis, supports investigations, and enables competent authorities to identify criminal activity and related networks.

Accordingly, reporting entities should seek to ensure that STRs are complete, accurate, and sufficiently detailed to enable the KwFIU to understand the nature of the activity being reported and the basis for the reporting entity's suspicion.

6.12 What Makes a High-Quality STR

A high-quality STR should clearly explain the circumstances that gave rise to suspicion and provide sufficient information to allow the KwFIU to understand the transaction, the parties involved, and the reporting entity's concerns.

The objective of an STR is not simply to describe events or reproduce transaction records, but to explain why the reporting entity considers the activity to be suspicious. Accordingly, STRs should present relevant facts in a logical and coherent manner and clearly distinguish between factual information and the reporting entity's analysis and observations.

Where some information is unavailable or incomplete, reporting entities should submit the STR based on the information reasonably available at the time and should not delay reporting solely to obtain additional details.

6.13 Analytical Narrative

The narrative section is one of the most important components of an STR. A good narrative should explain not only what happened, but also why the activity is considered suspicious.

Rather than merely listing red flags or reproducing transaction details, reporting entities should describe the circumstances giving rise to concern and explain how the available information, customer behavior, ownership arrangements, source of funds, transaction structure, or other factors contributed to the formation of suspicion.

The narrative should be clear, concise, and written in a manner that enables a person unfamiliar with the transaction to understand the reasons for the report.

As a general guide, reporting entities should seek to address the following questions:

- **Who** is involved in the activity, including customers, beneficial owners, intermediaries, counterparties, and other relevant persons?
- **What** activity or transaction is considered suspicious?
- **When** did the relevant events occur?
- **Where** did the transaction take place?
- **Why** does the reporting entity consider the activity suspicious?
- **How** was the transaction conducted, financed, or structured?

Answering these questions will assist in producing clear and meaningful reports and will enhance the value of the information provided to the KwFIU.

6.14 Description of Value Flows

Reporting entities should, to the extent possible, describe how funds or value moved throughout the transaction. This includes explaining the source of funds, the method of payment, the movement of money between parties, and the role of any third parties involved in financing or facilitating the transaction.

When known, reporting entities should identify the origin and destination of funds, explain the use of loans, mortgages, cash, or other payment mechanisms, and describe any complex, unusual, or unnecessary financing arrangements.

A clear description of value flows enables the KwFIU to better understand the transaction and identify potential links to other suspicious activities or persons.

6.15 Identification of Related Activity

Suspicious activity often forms part of a broader pattern rather than an isolated transaction. Accordingly, reporting entities should identify and describe any related transactions, customers, beneficial owners, intermediaries, legal entities, or counterparties that may be connected to the activity being reported.

Where previous transactions, repeated patterns, common addresses, common representatives, or recurring parties are known, such information should be included in the STR. Information regarding associated transactions or relationships may significantly enhance the intelligence value of the report and assist the KwFIU in identifying broader money laundering or terrorist financing schemes.

6.16 Supporting Documentation

Supporting documentation can strengthen an STR by helping to substantiate the facts described in the report. Where available and appropriate, reporting entities should provide relevant records and documents supporting the information contained in the STR.

Such documents may include customer identification records, beneficial ownership information, transaction records, contracts, invoices, purchase agreements, financing documentation, bank records, correspondence, internal analyses, and any other documents relevant to understanding the activity being reported.

Supporting documentation should complement, and not replace, the analytical narrative section of the STR. The submission of documents without a clear explanation of their relevance may limit their usefulness. Reporting entities should therefore ensure that the narrative explains how the documents support the basis for suspicion.

Ultimately, the quality of an STR is determined not by the quantity of information submitted, but by the reporting entity's ability to clearly explain why the activity appears suspicious and to provide sufficient information to enable the KwFIU to understand, analyze, and act upon the information received.

7 POST-STR OBLIGATIONS

The submission of an STR to the KwFIU does not bring a reporting entity's anti-money laundering and counter-terrorist financing obligations to an end. STR forms part of an ongoing process of risk management and monitoring, and reporting entities are expected to continue exercising appropriate vigilance after an STR has been submitted.

The filing of an STR does not transfer responsibility for monitoring the customer or transaction to the KwFIU.

Reporting entities remain responsible for managing the risks associated with their customers and business relationships and for complying with their obligations under applicable laws and regulations.

7.1 Ongoing Monitoring

Following the submission of an STR, reporting entities should continue to monitor the customer relationship and any subsequent transactions in accordance with the customer's risk profile and the reporting entity's internal policies and procedures.

Particular attention should be given to subsequent transactions, changes in ownership arrangements, unusual payment methods, the involvement of additional parties, and any other circumstances that may indicate continuing or evolving suspicious activity.

The submission of an STR should not, by itself, result in reduced scrutiny. In many cases, the circumstances giving rise to suspicion may justify increased monitoring and the application of additional risk mitigation measures.

7.2 Risk Reclassification

The filing of an STR may indicate that the customer's risk profile differs from that initially assessed. Accordingly, reporting entities should consider whether the circumstances giving rise to suspicion warrant a reassessment of the customer's money laundering and terrorist financing risk.

Where appropriate, the customer may be reclassified as presenting a higher level of risk, resulting in the application of enhanced due diligence measures, increased monitoring, more frequent reviews, or additional management oversight.

Risk reclassification should be based on the facts and circumstances of each case and should be supported by appropriate documentation.

7.3 Follow-Up STRs

The submission of an STR does not necessarily satisfy all future reporting obligations relating to the customer or transaction. Where additional suspicious activity is identified, or where new information becomes available that materially changes the reporting entity's understanding of the activity previously reported, a follow-up STR should be considered.

Follow-up reporting may be appropriate where:

- Additional suspicious transactions are identified;
- New parties, beneficial owners, or intermediaries are discovered;
- Additional information regarding the source of funds or ownership arrangements becomes available;
- Similar suspicious activity continues after the initial report;
- Previously unknown links to other customers, entities, or transactions are identified.

Follow-up STRs may provide the KwFIU with valuable information regarding the evolution of suspicious activity and help identify broader money laundering or terrorist financing schemes.

7.4 Management of the Business Relationship

The submission of an STR does not automatically require the termination of the business relationship. Decisions regarding whether to continue, restrict, or terminate a customer relationship should be made in accordance with the reporting entity's risk appetite, internal policies, and applicable legal and regulatory requirements.

In some circumstances, it may be appropriate to continue the relationship subject to enhanced monitoring and additional controls. In other situations, the level of risk may justify limiting or terminating the relationship.

Reporting entities should ensure that such decisions are based on risk considerations and are appropriately documented.

7.5 Identification of Related Activity

Suspicious activity may form part of a broader pattern involving additional transactions, customers, beneficial owners, legal entities, intermediaries, or associates.

Accordingly, reporting entities should continue to assess whether there are connections between the activity previously reported and subsequent transactions or relationships.

Information regarding linked transactions, recurring counterparties, common ownership structures, or other related activity should be considered when determining whether further internal review or additional reporting is required.

7.6 Tipping-Off Risks

Reporting entities should be aware that the submission of an STR and any related internal reviews are subject to strict confidentiality requirements. It is prohibited to disclose to a customer or any third party that an STR has been submitted, that a transaction or customer is under review, or that information has been provided to the KwFIU. Such disclosures, commonly referred to as "tipping off," may compromise investigations and are prohibited by law.

Tipping off may occur through direct or indirect actions or statements. Examples include informing a customer that they have been reported, suggesting that law enforcement authorities are interested in the transaction, or behaving in a manner that may reasonably alert the customer to the existence of an STR or internal investigation.

The prohibition against tipping off does not prevent reporting entities from conducting customer due diligence, requesting additional information, applying enhanced due diligence measures, delaying or refusing transactions where appropriate, or terminating a business relationship in accordance with internal policies. However, these actions should be carried out in a manner that does not reveal the existence or possible submission of an STR.

Reporting entities should ensure that access to STR-related information is restricted to personnel with a legitimate need to know and that internal procedures are in place to preserve the confidentiality of STRs and related records.

Maintaining confidentiality and avoiding tipping off are essential to protecting the integrity of financial intelligence and supporting the effective investigation and prosecution of money laundering and terrorist financing offenses.

8 ROLE OF THE KWFIU

The legal basis for the KwFIU is Article 16 of Law No. 106 of 2013, whereafter a unit called the "Kuwait Financial Intelligence Unit" shall be established. The KwFIU is an independent legal person and serve as the agency responsible for receiving, requesting, analysing, and disseminating information concerning suspected proceeds of crime or funds related, linked to or to be used for money laundering or terrorism financing. The KwFIU is not a law enforcement body but rather an administrative authority.

STRs submitted to KwFIU need to be communicated via a digital platform called GoAML, that all reporting entities in Kuwait are obliged to use.

The KwFIU conducts strategic analysis of important topics related to money laundering and terrorist financing. The KwFIU also conducts operational analysis of the STRs received from dealers in Precious Metals and Stones (DPMS) and other professions comprised by law 106 of 2013, not least the financial sector. When the operational analysis made by the KwFIU confirms the suspicion of money laundering or terrorist financing, it follows from Law no. 106 of 2013 that a dissemination report has to be sent to the Public Prosecutor's Office (PPO). Often the PPO would then decide that the Money Laundering Unit or the Terrorist Financing Unit of the Ministry of Interior (MOI) should carry out the preliminary investigation, including collection of evidence, whereafter the PPO will decide whether to prosecute or not.

The KwFIU is also responsible for identifying high-risk countries and prescribe the measures to be applied in relation to such countries.

The KwFIU is authorised to obtain from any person subject to the reporting obligation in Law no. 106 of 2013 any additional information it deems necessary to carry out its functions.

ANNEX

DPMS Sector Red Flag Indicators

A. Customer Due Diligence (CDD), Customer Profile and Behavioral Indicators

1. The customer is highly secretive or evasive regarding the source of funds.
2. Providing incorrect or incomplete information regarding one or more parties to the transaction, including unverifiable addresses or unavailable contact information.
3. The source of the customer's funds is unusual, inconsistent with the customer's profile, or cannot be reasonably verified.
4. The customer appears to be acting on instructions from another person without adequately explaining the relationship.
5. Refusal, reluctance, or repeated delays in providing required CDD information or documentation.
6. Use of forged, fraudulent, altered, or otherwise unreliable identification documents.
7. Adverse media or other reliable information linking the customer or beneficial owner to criminal activity, money laundering, corruption, fraud, sanctions evasion, terrorist financing, or other serious offenses.
8. The customer is a PEP, family member, close associate, or related person for whom adverse information exists.
9. The customer is unable to clearly explain the purpose of the transaction or provides inconsistent explanations over time.
10. The customer demonstrates unusual concern regarding AML/CFT procedures, reporting obligations, or beneficial ownership requirements.
11. The customer repeatedly changes information previously provided during the transaction process.
12. The customer terminates discussions or abandons the transaction after being asked to provide source of funds, beneficial ownership, or other due diligence information.
13. The volume of the customer's purchases is inconsistent with the customer's usual transaction pattern.

14. The customer is relatively young, and the purpose of the purchase, the commercial rationale, the economic justification, or the reason for the sale is unclear.
15. The customer insists on completing the transaction with unusual urgency before the required procedures have been completed.
16. The customer purchases gold or jewelry without regard to the price, quality, or specifications, focusing solely on converting or exchanging their funds.
17. The customer exhibits unusual nervous behavior, sometimes accompanied by threats, in an attempt to prevent the employee from carrying out their duties relating to the application of Customer Due Diligence (CDD) measures, including verifying the customer's identity or requesting supporting identification documents.

B. Beneficial Ownership Indicators

1. The customer appears to be purchasing precious metals or precious stones on behalf of another person.
2. The use of intermediaries or legal persons to conceal the identity of the beneficial owner.
3. Difficulty in identifying the ultimate beneficial owner despite taking reasonable measures to do so.
4. The beneficial owner resides in another country that has no apparent connection to the transaction and is unable to provide an adequate explanation of the purpose of the transaction.

C. Entity Indicators

1. The purchaser appears to be using company assets for personal purposes.
2. Investment companies or legal persons are involved in the transaction without any apparent legitimate commercial justification.
3. Recently established companies with little or no operating history are used to acquire high-value goods.
4. Companies with no apparent connection to the precious metals and precious stones sector engage in large-value transactions.

5. The ownership structure comprises multiple layers of ownership spread across several jurisdictions without any apparent legitimate commercial purpose.

D. Source of Funds and Financing Indicators

1. Sudden or unjustified changes in financing arrangements.
2. Use of unusual sources of financing that are difficult to explain.
3. Financing of down payments by third parties unrelated to the transaction.
4. Requests to transfer the transaction proceeds to third parties unrelated to the transaction.
5. The customer is unable to adequately explain the source of funds used in the transaction.
6. Funds are received from multiple unrelated sources without any apparent legitimate financial justification.
7. Funds are received from other countries that have no apparent connection to either the customer or the transaction.
8. Large sums of money are deposited shortly before the transaction is executed without a clear source of funds.

E. Transaction Indicators

1. Side payments or undocumented arrangements outside the scope of the official transaction.
2. Multiple purchase or sale transactions conducted within a short period.
3. An attempt to purchase gold, precious stones or precious metals in cash despite the prohibition of cash transaction for the purchase or sale of such goods.
4. Repeated purchases or sales of gold accompanied by unjustified changes in its value.
5. An urgent sale of the commodity coupled with a request for part of the purchase price to be paid in cash.
6. Transactions lacking an economic rationale or involving significant unjustified losses.
7. Sudden changes in the identity of the purchaser shortly before completion of the transaction.

8. Requests to expedite transactions at prices significantly above or below market value.
9. Purchasing a commodity and immediately reselling it without any apparent legitimate commercial justification.
10. Transactions with values significantly higher or lower than comparable market transactions.
11. Acquisition of a commodity followed by rapid payment without a clear source of funds.
12. Repeated transactions involving the same group of individuals or companies.
13. A significant increase in purchases of precious metals and precious stones by an existing customer without a clear reason.
14. A customer purchases gold bullion through multiple structured transactions within a short period.
15. A customer requests the conversion of gold into bullion, or vice versa, without any apparent legitimate commercial justification.

F. Intermediary Indicators

1. Involvement of multiple intermediaries without any apparent commercial necessity.
2. One intermediary appears to be directing the transaction, while the customer's role is limited.
3. Instructions are received from parties other than the customer or the declared beneficial owner.

G. Geographic Risk Indicators

1. The purchaser or seller is from a high-risk jurisdiction.
2. Use of accounts, individuals, or legal entities located in high-risk jurisdictions.
3. Funds originate from, or are transferred through, multiple jurisdictions without any apparent legitimate commercial justification.

H. Network and Relationship Indicators

1. Multiple customers appear to be acting in a coordinated manner when purchasing or selling goods.
2. Multiple transactions involve common addresses, telephone numbers, beneficial owners, or representatives.
3. The same intermediaries repeatedly appear in transactions that are otherwise unrelated.
4. Parties that appear to be unrelated conduct transactions that appear to be coordinated or economically linked.
5. The customer is linked to previous suspicious transactions, suspicious transaction reports, investigations, or persons known to be associated with criminal activities.

DIRECTOR OF THE AML-CFT DEPARTMENT:

مروه بداح الجعيدان
مدير إدارة مكافحة غسل الأموال
وتمويل الإرهاب

12july2026