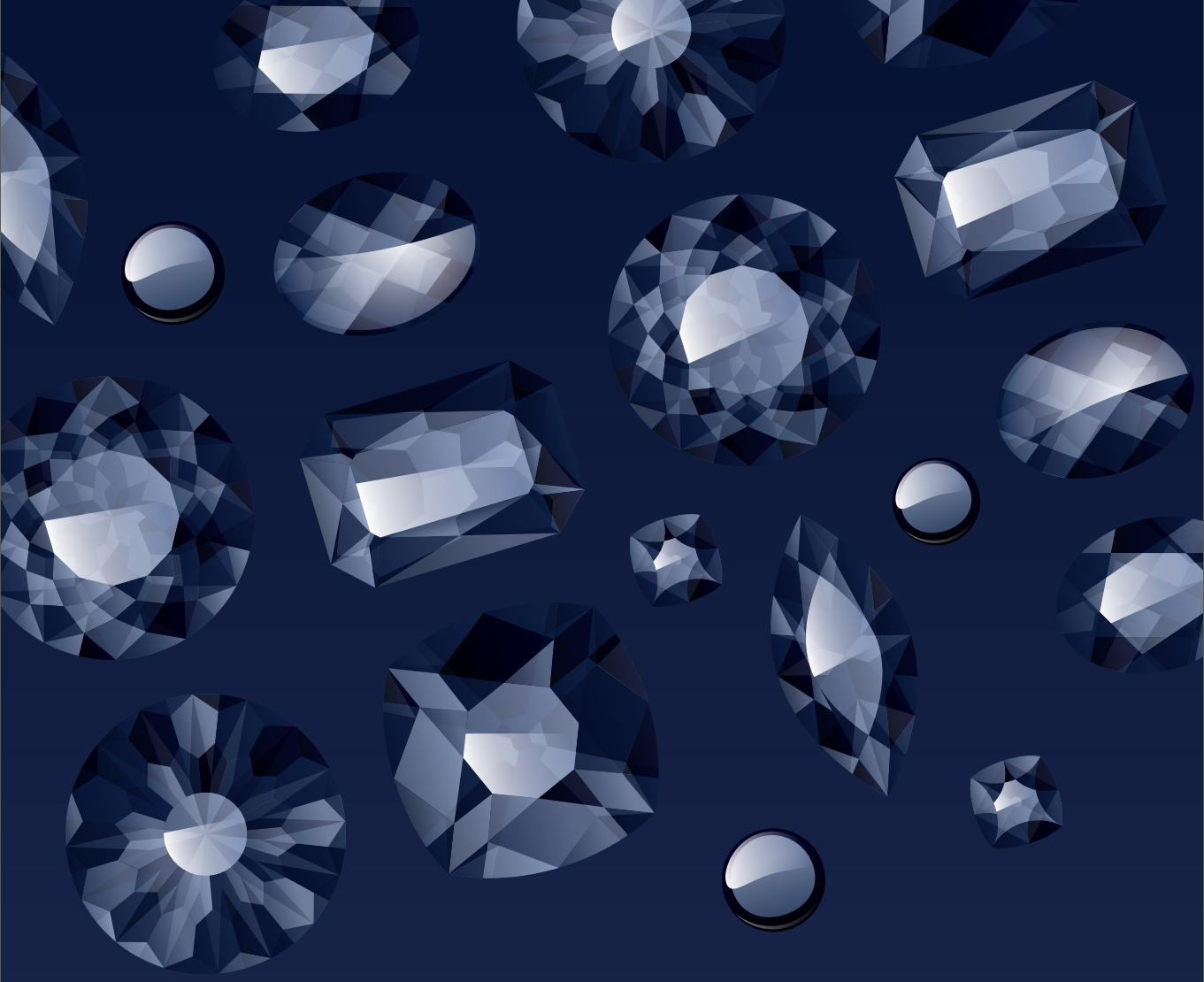


AML/CFT Compliance Guidance and Reporting obligations For Dealers in Precious Metals or Precious Stones

July 2020

وزارة التجارة والصناعة
Ministry of Commerce and Industry

وحدة المعلومات المالية
Financial Information Unit

Table of contents

Preamble

1- Scope of the Guidance 4

2- Purpose of the Guidance 5

3- Target audience and application of the Guidance 5

4- Money Laundering and Terrorism Financing Crimes 8

Chapter One: AML/CFT Compliance requirements for Dealers in Precious Metals or Precious Stones 13

1- Applying the Risk-Based Approach 14

2- AML/CFT Programme 17

3- Customer Due Diligence (CDD) 19

4- Enhanced Customer Due Diligence (EDD) 23

5- Simplified Customer Due Diligence 25

6- Beneficial Ownership 27

7- Politically Exposed Persons (PEPs) 30

8- Record Keeping 32

9- Reporting Suspicious Transactions 34

Chapter Two: Sanctions and Penalties Imposed on Dealers in Precious Metals or Precious Stones for Breach of AML/CFT Obligations 39

1- Penalities 40

2- Financial and Administrative sanctions 41

International References 42

Legal References 42

Useful links 42

Annexes **43**

Preamble

1- Scope of the Guidance:

The National Risk Assessment (NRA) of 2019[1] and the Sectoral Risk Assessment (SRA) conducted by the Ministry of Commerce and Industry (MOCI) on 2020, both identified the Precious Metals or Precious Stones sector as a higher risk sector in relation to ML/TF.The Qatar Central Bank has completed a sectroiel risk assessment (SRA) for the financial institutions .The results have concluded that the transactions conducted by dealers of precious metals , precious stones and gold with financial institutions are associated with a certain level of risk that requires FIs to implement efficient risk management framework to minimize any negative effects that such transactions might create[2] .

Precious metals such as gold, silver and platinium, or precious stones such as pearls, diamonds and jewels have a high value nature and are available in a relatively small size, which makes them readily transportable and easily bought and sold in various countries. Thus, such goods can be misused for exchanges and dealing operations by whoever is seeking to move funds through a cross border transportation since precious metals and precious stones, particularly gold, offer an alternative to criminals to store or proceed with a cross border movement of their assets and place proceeds illicitly in the financial system[3].

Gold is a precious metal, which holds its value throughout the years regardless of its shape whether as gold bars or gold articles, whether melted or smelted to being shaped. Thus, Gold is used for money laundering purposes, either obtained in an illicit manner (through theft or smuggling), where it constitutes proceeds of a crime and is therefore deemed to be considered as illicit funds, or is used as a money laundering means through the purchase of gold against illicit funds[4].

There are two broad characteristics of gold and the gold market which make it enticing to criminals. The first is the nature and size of the market itself which is highly reliant on cash as the method of exchange. The second is the anonymity generated from the properties of gold which make tracking its origins very difficult to do. These factors make gold highly attractive to criminal syndicates wishing to hide, move or invest their illicit proceeds[5].

Precious stones, in particular diamonds can also be traded around the world easily as the small size of diamond stones and their high value facilitate their concealment and transport and make it one of the most gems and jewels with the risk of being misused as a ML means. In some cases, it was noted that diamonds are used as a means to finance terrorist acts and groups.

However, gold remains the most traded precious metal in the State of Qatar comparing to other precious metals or precious stones[6].

1- According to the NRA, Dealers in precious metals and stones sector is one of the highest-risk channels used to launder the proceeds of crime.
2- Guidance on Business relationships with dealers in precious metals and stones and gold, QCB , May 2020.
3- FATF REPORT, Money Laundering / Terrorist financing risks and vulnerabilities associated with Gold, July 2015.
4- MENAFATF -DNFBPs in relation to AML/CFT – 10 November, 2008
5- FATF REPORT, Money Laundering / Terrorist financing risks and vulnerabilities associated with Gold, July 2015, p6
6- QCB Guidance to Management of risks related to Dealing with Traders in Precious Metals and Precious Stones -2019 , Guidance on Business relationships with dealers in precious metals and stones and gold, QCB , May 2020

2- Purpose of the Guidance

This joint Guidance[7] is designed to provide Dealers in Precious Metals or Precious Stones (DPMS) with a clear and simplified overview of their AML/CFT requirements under Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing, including the requirement to report any transaction suspected to be related to money laundering (ML) and terrorism financing (TF).

This Guidance reflects the provision of AML/CFT Law No. (20) of 2019, the Decision of the Council of Ministers No. (41) of 2019 Promulgating the Implementing Regulations of the AML/CFT Law, and the Decision of the Minister of Commerce and Industry No. (48) of 2020 promulgating AML/CFT Rules for legal Auditors, Dealers in Precious Metals or Precious Stones and Trusts and Company service providers.

Moreover, since suspicious transaction reports (STRs) play a crucial role in the fight against money laundering and terrorism financing crimes, Qatar Finiancial Information Unit (QFIU), through this Guidance is committed to assisting Dealers in Precious Metals or Precious Stones to meet their reporting obligations and ensuring they file suspicious transaction reports of high quality.

The AML/CFT Section recently established under the Companies Affairs Department at the MOCI, by Decision No. (95) of 2019, is responsible for the supervision of the compliance of Dealers in Precious Metals or Precious Stones with their AML/CFT requirements stipulated in this Guidance, and proposing the administrative and financial sanctions against any one who violate the provisions of the Law, its Implementing Regulations and any relevant decisions or instructions.

3- Target audience and application of the Guidance

I. To whom shall the Guidance apply?

Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing defines Designated Non-Financial Businesses and Professions (DNFBPs) to include Dealers in Precious Metals or Precious Stones, in line with the FATF Recommendations.

This Guidance shall apply to any trader licensed to engage in an activity related to precious metals or precious stones, including:

- Production of gold in a variety of forms: gold bars of different karats or silver bars(scrap gold refining), gold coins, gold items, jewellery, jewels, or ancient artifacts swords and arms.

- Trade in jewellery, precious metals whether crafted or no, gold and silver jewelleries, diamonds, precious stones, pearls and silver products.

7- The joint Guidance is prepared pursuant to the memorandum of understanding conducted between the QFIU and MOCI on May 16, 2019 in view of implementing the provisions of law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing, ensuring interagency coordination and cooperation between the supervisor authorities, and with the aim of enhancing the national efforts in combatting money laundering and terrorism financing.

• Manufacturing gold and silver metals, gold jewelleries, precious metals, traditional jewelleries and jewels and related products

• Goldsmithery, silversmithery and jewels smithery.

• Repairing jewels, jewellery and adornment.

• Leasing Jewels

Precious metals include gold, silver and platinum whether crafted (in its finished form) or half crafted (unfinished), coins or bars (not crafted gold, silver or platinum).

Precious stones of high value include diamonds, natural or cultured pearls, natural stones and synthetic gemstones.

This Guidance shall apply to Dealers in Precious Metals or Precious Stones operating in the State of Qatar, whether as individual businesses or commercial companies, and to all their foreign and domestic branches and majority-owned associates.

II. when are Dealers in Precious Metals or Precious Stones subject to AML/CFT requirements?

Dealers in Precious Metals or Precious Stones are subject to AML/CFT requirements **when they conduct a cash-based transaction with a value equal to or exceeding fifty thousand Riyals (QR 50.000),** whether the transaction is carried out in a single operation or in several operations that appear to be linked.

Dealers in Precious Metals or precious Stones who do not engage in cash transactions under any circumstances are not legally required to comply with these guidelines. However, Dealers who occasionally conduct cash transactions at or above the threshold, must maintain an AML/CFT program, including the appointment of an AML/CFT officer and training for staff. But they only need to apply the CDD and Recordkeeping measures described in this guidance when engaged in cash transactions meeting the description above.

Basically, under Qatari law a Dealer in Precious Metals and Stones qualifies as a DNFBP only when it engages in a cash transaction above the threshold. So technically, when it engages in a cash transaction worth 40,000 riyals, it doesn't have to apply any of the requirements in the Law. But there are elements of the requirements that you can't "turn off" and "turn on" from transaction to transaction. So, even if a month goes by where you don't engage in any qualifying transactions, you still need to have a compliance officer, train your staff, have a risk assessment in place. But you can omit Customer Due Deligance (CDD) on individual cash transactions that don't meet the threshold. These requirements will be discussed in greater detail below.

Detecting Linked or Structured Transactions

Criminals are aware that cash transactions of fifty thousand Riyals or more are subject to controls. For that reason, they may seek to avoid scrutiny by making multiple smaller purchases or sales of gold or precious metals, a practice known as structuring. Dealers in precious metals and stones must be alert to this tactic. Signs that a customer is seeking to avoid scrutiny include:

• The customer works hard to keep the transaction just under QR 50,000, such as by making minor adjustments to the purchase;
• The customer is set to buy a certain item until he hears the price, or until the seller begins to ask required questions, and then buys something quite different that is just under the threshold;
• The same customer visits the store every other day for a week and makes a purchase or sale of less than QR 50,000;
• Different customers make purchases below the threshold and have them delivered to the same household, or the same person comes to take possession of a series of purchases made by others.

4- Money Laundering and Terrorism Financing Crimes:

- **What is Money Laundering ?**

Article (2) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing stipulates "Whoever intentionally commits any of the following acts shall be deemed to have committed money laundering offence:

1. Conversion or transfer of funds, knowing that they are proceeds of a crime or an act of participation in the said crime; with a view to concealing or disguising the illicit source of funds or assisting any person involved in the commission of the crime to evade the legal consequences of his actions.
2. Concealment or disguise of the true nature, source, location, disposition, movement, ownership or the rights of funds, knowing that they are the proceeds of a crime.
3. Acquisition, possession or use of funds, knowing, at the time of receipt thereof, that they are the proceeds of a crime.
4. Participation in, association with or conspiracy to commit, attempt, or aid, abet, facilitate, counsel in, cooperate in, or contribute to the commission of any of the acts stipulated in this Article.

The Money Laundering crime should be considered as an independent crime of the predicate offence. When proving that funds are the proceeds of crime, it shall not be necessary that a person be convicted of a predicate offence

The punishment of the persons committing the predicate offence shall not prevent their punishment for the money laundering crime."

Considering this Article, the money laundering crime may have the following general characteristics:

1. Money laundering crime is an ancillary offence or a crime of consequence: refers to a ML crime committed following the commission of a principal offence, which generates proceeds used to commit the money laundering crime. This principal offence is defined as the predicate offence[8]

2. the money laundering offence is an independent crime of the predicate offence: It is not required that a person be convicted of a predicate offence to be traced for a money laundering crime and punishment for committing a predicate offence shall not prevent punishment for the money laundering crime.

3. Any funds or proceeds may be laundered and consequently the underlying conduct is criminalized: any funds or assets (whether physical or non-physical, movable or immovable), including the revenue, income, or interest derived or obtained, directly or indirectly, from committing a predicate offence may be an underlying money laundering crime.

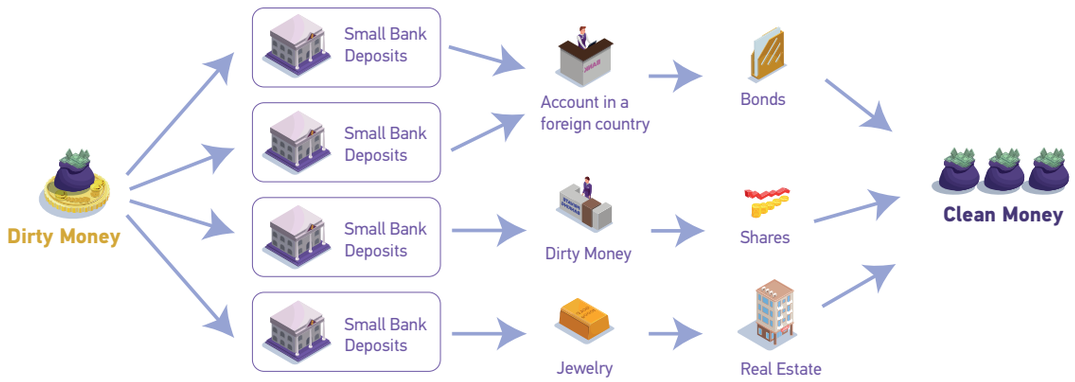
4. The money laundering Offender may be: (a) either the perpetrator of the predicate offence: in this case, he proceeds by his own with concealing the true criminal source of funds; (b) or any other person who assists (the perpetrator of the predicate offence) for the purpose of integrating the proceeds of crime into the formal economy.

5. Sanctions imposed for committing a money laundering crime: Any person who commits any of the money laundering crimes stipulated in Article (2) of the Law No. (20) of 2019 on Combating

8- Article (1) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing defines the predicate offence as any act constituting a misdemeanour or a felony under any law in force in the State, whether committed inside or outside the State, whenever it generates funds and is an offence punishable by law in both countries.

Money Laundering and Terrorism Financing, shall be sentenced to imprisonment for a term not exceeding ten (10) years, and a fine not less than (QR 2.000.000) two million Qatari Riyals and not more than (QR 5.000.000) five million Qatari Riyals, or twice the value of the money laundered, whichever is greater[9] .

- **Money Laundering Stages:**



Crimes such as drugs and arms trafficking, corruption and bribery can generate huge amounts of proceeds to perpetrators who seek to conceal or disguise their illicit sources through money laundering in order to benefit from such proceeds:

1- Placement: At this stage, the money launderer disposes of the proceeds of the crime:

- by placing the proceeds in the financial system usually through a financial institution:

- **Either** by breaking up large amounts of cash into smaller amounts of less than fifty thousand Riyals (QR.50,000) to avoid raising any suspicions and scrutiny, and then depositing such amounts into different accounts held by different persons at different times and different branches of the financial institution (s) (Smurfing/schtroumphage).

- **Or** by converting banknotes with a low value to banknotes with higher value, or to foreign currencies, or financial instruments such as checks, payment orders, to facilitate their physical cross border transportation.

- Moreover, the money launderer may place the proceeds of the crime by buying real estates and movable assets like gold, precious metals and precious stones directly and with large amounts, or by structuring the purchases to avoid raising any suspicions, in particular when the conducted financial transactions are not proportionate to the usual size or pattern of transactions of similar customers.

- In addition, proceeds of crime are not always in cash, they can include the income, interest, revenue or other product, whether or not it has been transferred in whole or in part into properties or investment proceeds.

9- Article (78) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing.

2- Layering: After the placement of the proceeds of the crime, the money launderer disguises or conceals the illicit source by performing a series of complex operations and transfers that prevent the detection of the source of the proceeds, such as by carrying out services, concluding fictitious contracts and bills and establishing front companies; or by selling or purchasing gold, precious metals and precious stones without a business purpose, which make traceability of the illicit source of funds very complicated.

3- Integration: at this stage, the money launderer injects the proceeds of the crime into licit economic activities to give them an apparently legitimate source. Following successful integration, funds can be easily demonstrated to the profits of a legitimate business, proceeds from the sale of legitimately acquired precious metals or stones, etc. Once integration has successfully taken place, it is very difficult and even impossible to identify funds as the proceeds of crime.

• What is terrorism financing?

Article (3) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing stipulates "Whoever intentionally, by any means, directly or indirectly, with an unlawful intention provides or collects funds to be used, or while knowing that they are to be used, in whole or in part, in any of the following, shall be deemed to have committed a terrorist financing offence:

1. To carry out a terrorist act(s);

2. By an individual terrorist or by a terrorist organization, even in the absence of a link to a specific terrorist act or acts;

3. To finance the travel of individuals to a state other than their state of residence or nationality, for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training;

4. To organize or direct others to commit or attempt to commit any of the acts stipulated in this Article.

5. To participate; collude; aid, abet, facilitate, counsel in, cooperate in, conspire to commit or attempt to commit any of the acts stipulated in this Article.

The terrorism financing offence extends to any funds, **whether from a legitimate or illegitimate source, regardless of whether the funds were actually used to commit or attempt to commit a terrorist act, or are linked to a specific terrorist act.**

The terrorism financing offence shall be deemed to have been committed, irrespective of whether the person charged with committing the offence is present in the same country or where the terrorist or terrorist organization is located or where the terrorist act was committed, or would be committed or in any other State.
The terrorism financing offence shall be considered a predicate offence of money laundering."

As stated above, terrorism financing is to provide or collect funds, whether from a licit or illicit source, to be used:

- for perpetrating a terrorist act(s);

- by a terrorist or terrorist entity, even in the absence of any relation with a specific terrorist act(s).

The terrorism financing offence extends to any funds, that are assets or property of every kind, whether physical or non-physical, tangible or intangible or movable or immovable. It is important to be aware that "funds" does not just mean money. Providing anything of value to a terrorist or a terrorist group—or collecting it with the intention of providing it—is a terrorist financing crime. This can include providing food, housing, medical supplies, weapons, and computers—not just cash or electronic transfers.

Article (79) of the same Law stipulates "any person who commits any of the terrorism financing crimes stipulated in Article (3) of this Law shall be sentenced to imprisonment for a term not exceeding twenty (20) years, and a fine not less than (QR 5.000.000) five million Qatari Riyals and not more than (QR 10.000.000) ten million Qatari Riyals, or twice the value of the financing provided for, whichever is greater".

• What is the difference between money laundering and terrorism financing crimes?

Money laundering crime	Terrorism Financing Crime
The crime is **independent** of the predicate offence	The crime is a **predicate** offence to the money laundering crime
The crime is **subsequent** to the predicate offence	The crime is **often prior** to the terrorism crime
The laundered money is **the proceeds of the predicate offence**	Funds used in terrorism financing can be **licit** (fundraising, etc.) or illicit (proceeds of drugs trafficking, etc.).

• Is the Legal Person punished for ML/TF crime?

Article (77) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing stipulates "a legal person, on whose behalf or for whose benefit any of the crimes stipulated in this

Law has been committed by any natural person, acting either individually or as part of an entity of the legal person, or serves in a leading position therein, or represents the legal person, or is authorized to take decisions or exercise control on behalf of the legal person, and acts in such capacity, shall be sentenced to a fine not less than (QR 4.000.000) four million Qatari Riyals and not more than (QR 8.000.000) eight million Qatari Riyals, or threefold the maximum fine applied to such offence, whichever is greater.

The above should not prevent the punishment of the natural person, perpetrator of the crime, with the corresponding penalty prescribed by this Law.

The Court may order that the legal person be prohibited, either permanently or temporarily, from directly or indirectly carrying on certain business activities, or be subjected to judicial supervision, or to close permanently or temporarily the premises used for perpetrating the offence, or to dissolve and liquidate his business. The Court may also order that the judgment issued against the legal person in relation thereto, be published in two daily newspapers at the legal person's own expense".

Chapter One: AML/CFT Compliance requirements for Dealers in Precious Metals or Precious Stones

1- Applying the Risk-Based Approach:

Risk-Based Approach is a series of measures and procedures that aims at identifying, assessing, understanding and mitigating Money Laundering and Terrorism Financing risks, in order to allocate sufficient resources to focus on prioritized areas such as highrisk activities, customers or transactions, to achieve effectiveness.

I. How do Dealers in Precious Metals or Precious Stones assess their ML/TF risks?

To comply with the AML/CFT requirements, Dealers in Precious Metals or Precious Stones should:

1. Develop and apply a risk assessment for their business. The goal of the risk assessment is to identify, assess and understand the dealer's money laundering and terrorism financing risks. The risk assessment should be appropriate to the size and nature of their business: larger businesses will need a more in-depth and comprehensive risk assessment.

2. The risk assessment must consider the following:

- **Size of their business:** Is the business a single person? A single store? Multiple stores in different countries, with a large staff? Larger businesses may be higher risk because it's more difficult to track customer activity and to get to know your customers.

- **Nature of their business:** Certain parts of the gold and precious metals sector are higher risk than others. Sale in gold bullion and in loose stones is considered the highest risk because these items are most attractive to illicit actors. They can be easily hidden and carried across borders, and their value is likely to be the same all over the world[11] . In contrast, finished jewellery, particularly costume jewellery, is considered to be lower risk because the resale value is more unpredictable and because it is more difficult to move large values through a relatively small object.

- **Risks identified in the National Risk Assessment (NRA):** The NRA discusses the primary proceeds-generating crimes in Qatar, as well as ways in which criminals may seek to launder the proceeds of those crimes or terrorist financiers may seek to move funds. Dealers in precious metals and precious stones must be aware of the findings of the NRA and consider whether any of these apply to their business, including their customer base.

- **Risk factors associated with the customer base:** The risk of the customer base may be high if many of a business's customers or suppliers are high-ranking officials or one of their family members and close associates (known as politically exposed persons and discussed below) or reside in high-risk jurisdictions or was not subject to the identity verification process (i.e. non-face to face transactions). Customers or suppliers that are other dealers in precious metals or stones may also be higher risk, as are customers that are legal person or arrangement, whose structure or nature makes it difficult to identify the beneficial owners. Or a customer attempting to obscure understanding of his business or transactions through shell or front companies, or companies with a complex ownership structure or companies managed over different countries without any apparent economic reason, or a customer who is a legal person and operates a considerable part of his business in, or have branches in, countries that pose high-risk.

- Businesses should also consider how well they know their customers—a business that serves a small group of customers who have been patronizing the dealer for many years may be lower risk than a business that has a large and constantly changing customer base, because in the first case it's easier to know your customers' backgrounds, their businesses, and what they do with your products. That said, simply because you have known a customer for years doesn't mean he or she is low risk.

- In assessing customer risk, dealers must consider not just their direct customers, but the people who own and control their legal person customers, known as "beneficial owners" (discussed below).

- **Risk factors associated with jurisdictions and geographical areas:** A business may be **higher** risk factors if it frequently conducts transactions associated with jurisdictions identified by credible and reliable source documents (such as by NAMLC, or in Financial Action Task Force (FATF) statements), as having ineffective AML/CFT regimes or high level of corruption and other criminal activities. An association with jurisdiction could mean that the business sources raw or finished goods from that jurisdiction, has suppliers there, or works with intermediaries or customers who are based in that jurisdiction, or has business dealings there. On the other hand, **the risks may be lower** if the transaction is related to jurisdictions which have effective AML/CFT regime or identified by credible and reliable sources as jurisdictions with low propensity for corruption and other criminal activities or identified by reputable bodies and organizations in the mutual evaluation process.

- **Risk factors associated with products, services, transactions and professional practices:** Certain products and services are considered to be higher risk for ML/TF because they make it easier for illicit actors to abuse your business. The physical characteristics of the product offered are also a factor to consider. Products that are easly portable and which are unlikely to draw the attention of law enforcement are at greater risk of being used in cross border money laundering. For example, diamonds are small, light in weight , not detected by metal detectors , and a very large value can be easly concealed[12] . Beyond the nature of the business and the products you sell, these could include sales made over the internet (or any other arrangement in which you never come face to face with your customer); products or services that favour anonymity or that are provided "no questions asked;" cash transactions of any value, because the funds did not travel through a regulated financial institution; and transactions which involve new or developing technologies, such as accepting virtual assets (cryptocurrencies, such as Bitcoin).

11- RBA Guidance for dealers in precious metals and stones , FATF 17 June 2008, p 23

12- RBA GUIDANCE dor dealers in precious metals and stones, FATF 17 june 2008 , p 24

3. You must update your risk assessment regularly, as discussed below. In particular, you must update your risk assessment before beginning to offer new products or services or using new delivery channels or new technologies.

II. What is the Methodology adopted by Dealers in Precious Metals or Precious Stones to address and mitigate their ML/TF risks?

Dealers in Precious Metals or Precious Stones must rely on an appropriate methodology that addresses the risks they face when applying their approach to mitigate ML/TF risks (risk assessment methodology), which is particularly based on the following:

- Identifying the nature of the business relationship with each customer and understanding its purpose.

- Assessing the risk profile of the business relationship by rating that relationship.

Dealers in Precious Metals or Precious Stones must develop a risk assessment methodology that will help them to identify and detect any changes in their ML/TF risks. The methodology must be updated, as necessary. DPMS should take into account the findings of the risk profile of the business relationship when identifying the due diligence and ongoing monitoring measures that will be applied to the customer.

III. What should Dealers in Precious Metals or Precious Stones do with the results of their ML/TF risk assessments?

Dealers in Precious Metals or Precious Stones should:

1. Document their ML/TF risk assessments and any basic information to be able to demonstrate their basis.

2. Document the basis and sources they used to identify, assess and understand their ML/TF risks taking into consideration the National Risk Assessment and any other relevant source to identify such risks.

3. Monitor the implementation of the Risk Assessment's findings and update the risk assessment on ongoing basis.

4. Provide relevant periodic reports to the AML/CFT Section at the MOCI within the set timeframe and upon its request.

2- AML/CFT Programme

Dealers in Precious Metals or Precious Stones should:

1. Develop an AML/CFT programme that includes internal policies, procedures and controls that are commensurate with the risks identified, taking into consideration the size, complexity and nature of the business.

2. Implement the programme effectively to manage and mitigate their risks taking into consideration the nature and size of their businesses.

3. Review, update and enhance the programme, when necessary.

4. Apply the programme to branches and majority-owned associates, whether inside or outside the State of Qatar.

5. Provide a copy of the AML/CFT programme and the annual report of the Compliance Officer once a year to the AML/CFT Section at the MOCI, and any other supporting documents that may be requested for this purpose.

I. What does the AML/CFT Programme include?

1- Appropriate compliance management arrangements including the appointment of a compliance officer and his Deputy at the management level.

The appointed Compliance officer is responsible for overseeing and managing the regulated entity's compliance with the AML/CFT requirements stipulated in the AML/CFT Law, its Implementing Regulations and the AML/CFT Rules for Auditors, Dealers in Precious Metals or Precious Stones and Trusts and Company Service Providers. The Compliance Officer prepares and submits the Suspicious Transaction Reports (STRs) to the QFIU. He is responsible for overviewing the effective implementation of the AML/CFT Programme (ensuring that appropriate policies, procedures, systems and controls are established and developed on a regular basis, risk assessments, reviews and testing are conducted to ensure the effectiveness of this Programme).
The Compliance Officer also acts as a focal point for communication between the Dealer in Precious Metals or Precious Stones, the AML/CFT Section and other competent authorities in AML/CFT related matters
If the Dealer in Precious Metals or Precious Stones conducts his activity as a commercial company, he should appoint one of the employees to act as a compliance officer to manage compliance with the AML/CFT requirements, particularly to prepare and file STRs with the QFIU. If the Dealer in Precious Metals or Precious Stones conducts his activity as an individual business activity, he should personally undertake the senior management and the compliance officer responsibilities or may appoint one of his employees as a compliance officer (Article 2 of AML/CFT rules).
In all cases, the compliance officer must be entrusted with all relevant powers and competences to perform his duties effectively, reasonably and independently, as set forth in the AML/CFT Rules for Chartered Accountants, Dealers in Precious Metals or Precious Stones, Trusts and Company Service Providers of 2020.
The name and full data of the compliance officer and his Deputy must be reported to the AML/CFT Section and the QFIU through a form available in the AML/CFT section website.

2- Adequate screening procedures to ensure high standards when appointing employees:

DPMS should develop adequate screening procedures to ensure high standards and integrity of their employees and officers as set forth in the AML/CFT Compliance Rules.

Enhanced screening procedures must be adopted in particular for higher impact individuals, such as employees engaging in a direct activity with the customer; or employees conducting and overseeing the financial transactions of the Dealers in Precious Metals or Precious Stones. To comply with this requirement, the screening procedures before appointment or employment must, as a minimum: obtain and confirm references about the individual; confirm the individual's employment background and qualifications; seek and verify information or details about any criminal convictions of, or regulatory actions against, the individual.

3- Ongoing training programme for employees:

Dealers in Precious Metals or Precious Stones must develop and design an appropriate ongoing training programme for their officers and employees to maintain their knowledge of international and domestic AML/CFT legal frameworks; and to ensure they are up-to-date with internal policies, regulations, procedures and controls adopted by DPMS to manage and mitigate ML/TF risks.
Training must assist employees to keep abreast of any ML/TF patterns or trends, must ensure they are trained to make the related STRs, and must inform appropriate employees of the importance of conducting CDD measures and ongoing monitoring.
Training should be tailored to the employee's role in the organization; for instance, employees on the sales floor may need to receive somewhat different training than those in the back office. The training programme must be documented and updated on a regular basis.

4- Independent audit and review function to test Compliance with the AML/CFT systems:

the testing must include in particular the AML/CFT programme, the screening procedures for employees, record making and record keeping, in addition to the ongoing monitoring in relation to customers; aiming at identifying gaps, deficiencies and shortcomings for future remedial actions. The testing must be conducted at least once every two (2) years by an independent internal or external auditor. A record of the testing results must be made and kept and a copy of this record must be provided to the AML/CFT Section at the MOCI by 31 July 2021 and every two (2) years thereafter.

3- Customer Due Diligence (CDD):

Customer Due Diligence is a series of measures taken to ensure that Dealers know and fully understand their customers. It includes the following: identifying and verifying the customer's identity using reliable, independent source documents, data or information; determining whether the customer is acting on behalf of another person, and verifying if the latter is authorized to do so, including identifying and verifying his identity; understanding the pattern and nature of the customer's business activity, the purpose and intended nature of the business relationship; and establishing the legal status of the customer, whether he is a natural person or legal person or legal arrangement

I. When Customer Due Diligence is required:

- Dealers in Precious Metals or Precious Stones should conduct CDD when:

1. Establishing business relationships involving the use of cash.

2. Conducting cash transactions with a value equal to or exceeding fifty thousand (QR. 50.000), whether as a one-off transaction or in several operations that appear to be linked.

3. There is a suspicion of money laundering or terrorism financing irrespective of the amount of the operation.

4. They have doubts about the veracity and adequacy of previously obtained customer identification data.

- Dealers in Precious Metals or Precious Stones should conduct CDD **before establishing a business relationship with the customer or conducting a one-off transaction**. However, CDD measures may be completed at a later stage **during the business relationship** in the cases specified by the AML/CFT Section at the MOCI, provided that:

1. The customer's identity is verified, as soon as practicable

2. This is necessary in order not to interrupt the normal conduct of business.

3. There is little risk of money laundering or terrorism financing and any risks are effectively managed; and in cases of imposing restrictions with regard to the number, types and amount of transactions that may be conducted, provided that CDD is completed as soon as practicable, after contact is first established with the customer

- If the Dealer in precious metals or precious metals conduct CDD measures after the establishment of the business relationship, he must document each instance and be prepared to demonstrate to the AML/CFT section at MOCI that delayed CDD was appropriate and justified in that context

II. What are the CDD measures to be conducted by Dealers in Precious Metals or Precious Stones, when the transaction exceeds fifty thousand Riyals (QR. 50,000)?

• Dealers in Precious Metals or Precious Stones are prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

• Dealers in Precious Metals or Precious Stones are required to undertake CDD measures as mentioned above, to identify and verify the customer's identity, legal status, activities, the purpose and nature of the business relationship and the beneficial owner/s of the customer. Those measures shall particularly include the following:

1. Identify and verify the identity of customers using reliable, independent source documents, data or information.

2. Identify the person who is acting on behalf of the customer and verify that any person purporting to act on behalf of the customer is so authorised in conformity with the relevant rules and laws.

3. Identify the customer's beneficial owner(s) at the 20% threshold and take reasonable measures to verify the identity of the beneficial owner using reliable independent source documents, information or data, such that the DPMS are satisfied that they know who the beneficial owner is (See Section 6 below for a full discussion of beneficial ownership).

4. Obtain information on and understand the intended purpose and nature of the business relationship or transaction.

5. Identify the nature of the customer's business; and for customers who are not individuals (such as companies), understand their ownership and control structure and verify the identity of the beneficial owner.

6. Obtain and verify additional information based on the risk factors associated with the customer or with the customer's businesses and transactions.

7. Review and update the records of the customer on a regular basis, to ensure that documents, data and information collected using CDD are kept up-to-date and relevant, particularly for high-risk categories of customers.

8. Scrutinize transactions conducted throughout the course of the business relationship on a regular basis, to ensure that the transactions are consistent with the Dealers in Precious Metals or Precious Stones' knowledge of the customers, their business and risk profile, including where necessary, the source of their wealth and funds.

• DPMS shall ensure the veracity and adequacy of previously obtained data as stated above, using reliable, independent source documents, data and information.

• DPMS should identify and verify the identity of the customer using reliable, independent source documents, data or information, and shall at least obtain the following information:

1.For customers that are natural persons: name of the person as registered in the official documents (full identity and photograph), residence address or domestic address, date and place of birth, and nationality.
For example: name, date of birth, and nationality of the customer by verifying a valid passport or identification card with a clear photograph. The customer's place of residence can be verified based on a leasing contract, Kahrama bill or a letter by the employer.

2.For customers that are legal persons or legal arrangements: name, legal form[13] and proof of existence of the person; the mandates, declarations, resolutions and other sources of power that regulate and bind the legal person as well as the names of the relevant persons holding a senior management position in the legal person or arrangement; the address of the registered office and, if different, its principal place of business.

3. For customers that are legal persons or legal arrangements: the dealer in precious metal or precious stones shall understand the customer's ownership and control structure; and shall verify the identity of the beneficial owners.

III. Can Dealers in Precious Metals or Precious Stones rely on third parties to conduct CDD?

- DPMS may rely on third parties such as financial institutions and DNFBPs to conduct CDD measures to identify the customer, the beneficial owner and understand the nature of the business.

- DPMS remain the ultimate responsible for the proper conduct of CDD measures.

13- For example, if it involves a commercial company, it is required to take a legal forms stipulated in Article (4) of Law No. (11) of 2015 on Issuing Commercial Companies; such as Partnership company, Limited Partnership Company, Particular Partnership Company, Public Shareholding Company, Private Shareholding Company, Limited Partnership Company with Shares, Limited Liability Company.

- DPMS, when relying on third-party to perform the CDD measures as set out in the AML/CFT Law and it's implementing regulation, shall:

1. Immediately obtain from the third party necessary information in relation to the CDD measures and identification of the Customer.

2. Ensure that the third party will provide without delay and upon request a copy of every document relating to the customer and other documents in relation to such measures that Dealers in Precious Metals or Precious Stones would need if it were conducting CDD itself for the customer.

3. Verify that the third party is regulated and supervised and complies with the CDD measures requirements and maintains the records in conformity with this Law and the Implementing Regulations.

4. DPMS must have regard to any relevant findings published by international and regional organizations and foreign jurisdictions, as well as available information on the level of risks related to ML and TF in jurisdictions where the third party operates or is located, before deciding to rely on said third party.

5. Ensure that it has received from the third party all information about the customer obtained from the CDD conducted by the third party introducer for the customer that it would need if it had conducted the CDD itself.

IV. What should Dealers in Precious Metals or Precious Stones do when they cannot complete CDD because the client refuses to provide the information or when they discover that the customers' data are fictitious or incomplete?

DPMS should:
1. not establish or continue the business relationship with the customer, or carry out the transaction for the customer.

2. strongly consider filing an STR with the QFIU in relation to the customer, especially if the customer refuses to provide information, backs out of the process halfway through, or provides fictitious information.

3. be aware that providing false beneficial ownership information or concealing the interest of a Politically exposed Petrsons (PEP) in a transaction (see Section 7 below), may be a crime under Qatari law.

V. What should Dealers in Precious Metals or Precious Stones do when they suspect that the transactions are associated with money laundering or terrorism financing?

In cases where DPMS form a suspicion when establishing a business relationship with the customer, or in the course of such business relationship, or when carrying out occasional transactions, that those transactions are related to money laundering and terrorism financing, they should:
1. Identify and verify the identity of the customer and the beneficial owner, even if the customer is an existing customer or an occasional customer and regardless of any exemptions or thresholds.

2. If the dealer reasonably fears that asking too many questions will warn the customer of the dealer's suspicions, the dealer can skip CDD but must immediately make an urgent report to the QFIU.

3. File an STR with the QFIU.

4- Enhanced Customer Due Diligence (EDD):

I. When is enhanced CDD required?

DPMS should apply enhanced CDD:

1- For business relationships and transactions with customers from certain countries

- Countries identified by NAMLC as high-risk countries; and circulars about the vulnerabilities of their AML/CFT regimes are issued and published on NAMLC's website.

- Countries subject to a FATF enhanced due diligence requirement. Information about these countries will be published on NAMLC's website[14] .

14- See Circular No. (6) of 2020 for Auditors, Dealers in Precious Metals and Stones and Trust and Company Service Providers about High-Risk Jurisdictions Subject to A Call for Action by the Financial Action Task Force and Jurisdictions Under Increased Monitoring, attached to this guidance.

2- When ML/TF risks are high, especially in the following cases:

• Complex, unusual large transactions or unusual patterns of transactions that have no apparent or visible economic or lawful purpose.

• Non face-to-face purchase and sale transactions, direct or indirect, or transactions concluded using electronic means and instruments, as well as to other risks emerging from products and transactions that might favour anonymity and concealment of the source or identity[15].

• Purchase and sale transactions or transactions involving the power of attorney through non-resident customers in the State.

3- For other cases that are identified by NAMLC and the AML/CFT Section of the MOCI as high ML/TF risks for Dealers in Precious Metals or Precious Stones.

II. Enhanced CDD to be conducted by Dealer in Precious Metals or Precious Stones:

The goal of Enhanced CDD is to learn more about the customer or transaction in order to minimize the chance that the customer or transaction is involved in ML/TF. Therefore, Enhanced CDD should be tailored to fit the risk of the specific customer or transaction.DPMS should generally carry out the following enhanced measures, but may add others as appropriate:

1. Increase the frequency and intensity of the business relationship monitoring;
2. Obtain additional information about the customer including profession, volume of assets and information available through public databases and open sources;
3. Update on an ongoing basis the identification data of the customer and the beneficial owner, by undertaken reviews of existing records particularly for high-risk categories of customers;
4. Obtain additional information on the purpose and intended nature of the business relationship;
5. Obtain additional information on the customer's source of wealth and funds;
6. Obtain information on the purpose of the intended transactions or the conducted transactions;
7. Obtain senior management approval before establishing or continuing a business relationship;
8. Take enhanced measures to monitor the business relationship by furthering the intensity and degree of supervision, and identifying patterns of transactions that require additional scrutiny and review;
9. Make the first payment through an account in the customer's name in a bank that is subject to similar CDD measures.

15- see Circular No. (5) of 2020 on Dealers in Precious Metals or Stones in Terms of Implementation of Enhanced Customer Due Diligence for Non-Face-to-Face Transactions.

5- Simplified Customer Due Diligence:

I. When can Dealers in Precious Metals or Precious Stones conduct simplified CDD?

DPMS may conduct simplified CDD when all the following conditions are met:

1. If the risk factors of the customer or transaction identified in the National Risk Assessment are low;
2. If the risk factors of the customer or transaction identified in the self- assessment are low.
3. There is no suspicion of ML/TF.
4. There are no higher-risk factors, such as a link to a higher-risk jurisdiction, present.

II. What are the simplified CDD measures that Dealers in Precious Metals or Precious Stones can conduct?

Simplified CDD can consist of taking one or all of the following actions:

1. Verifying the identity of the customer and beneficial owner after the establishment of the business relationship.
2. Reducing the frequency of the customer's identification updates.
3. Reducing the intensity of ongoing monitoring and scrutiny of transactions based on a reasonable threshold

4. Limiting the collection of information, or the conduct of specific measures, to determine the purpose and intended nature of the business relationship and inferring instead the purpose and nature from the type of transactions carried out or from the business relationship established.

In any case where a dealer in precious metals or precious stones carries out simplified CDD, he must document the risk assessment and be prepared to demonstrate to the AML/CFT section at MOCI that the risk was appropriate and justified in this context.

6- Beneficial Ownership:

I. Who is the Beneficial Owner?

The Beneficial Owner(s) are:

1. The natural person who ultimately owns or controls a customer, through ownership interest or voting rights.

2. The natural person on whose behalf a transaction is being conducted, whether by proxy, trusteeship or mandate or by any other form of representation.

3. Any natural person who holds ultimate effective control over a legal person or arrangement, including any natural person exercising ultimate effective control by any means.

II. What are the Dealers in Precious Metals or Precious Stones' obligations in relation to the Beneficial Owner?

1. DPMS should identify and take appropriate and reasonable measures to verify the identity of the beneficial owner before establishing business relationships with the customer, using reliable, independent source documents, data or information until they are satisfied that they know who the beneficial owner is.
2. Where the customer is a legal person or legal arrangement, DPMS should understand the

customer's ownership and control structure and verify the identity of the beneficial owner in conformity with the criteria referred to below.

III. How to identify the Beneficial Owner?

Dealers in Precious Metals or Precious Stones must identify the beneficial owner as follows:

- **Identifying the Beneficial Owner of legal persons:**

1. Identify the natural person(s) who ultimately has an effective controlling interest of at least 20% of a legal person or voting rights.

2. If no individual can be identified as the beneficial owner of the legal person, or there is a doubt that a natural person who ultimately owns effective control is the beneficial owner under (1) above; or

3. If no natural person exerts control through ownership interests, Dealers in Precious Metals or Precious Stones must identify the natural person (s) exercising de facto or legal control in the legal person and arrangement through any means, whether directly or indirectly, over the executives, the general assembly, or the operations of the legal person, or any other control instruments.

4. In case no natural person is identified under (1), (2) and (3) above, Dealers in Precious Metals or Precious Stones should identify and verify the identity of the relevant natural person holding a senior managing position in the legal person (e.g. the legal representative of the commercial company).

- **Identifying the Beneficial Owner of legal arrangements:**

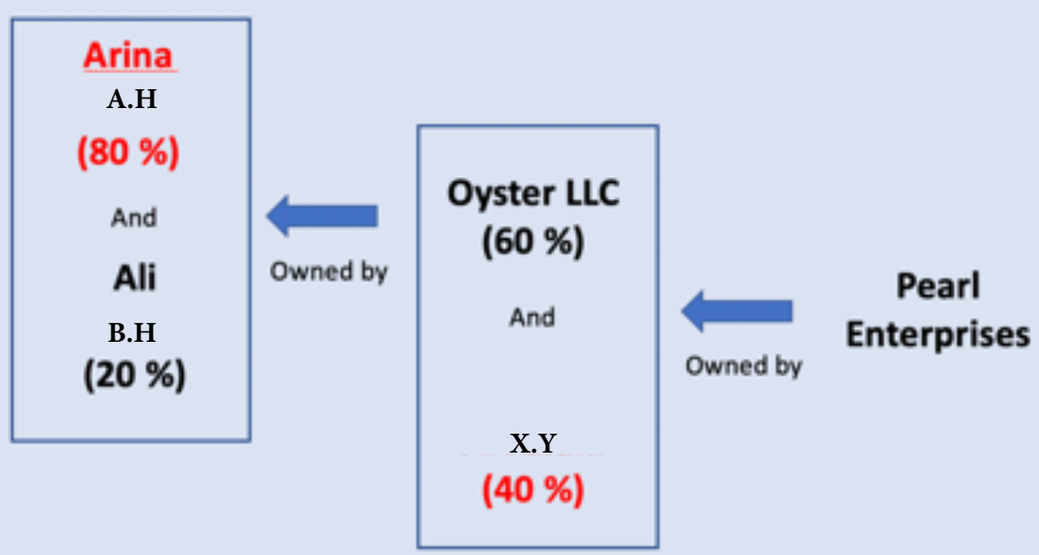
1-if the customer is a trust: identifying the settlor, the trustee and the protector (if any) and the beneficiaries or class of beneficiaries, and any other natural person exercising, directly or indirectly, ultimate effective control over the trust.

2-For other types of legal arrangements: identify the natural person in equivalent or similar positions.

3-Take the necessary procedures to determine whether a customer is acting as a trustee of a trust, or holds an equivalent or similar position in other types of legal arrangements.

Identifying Beneficial Owners

When your customer is an individual, conducting CDD on that individual should give you the information you need to understand the customer and the purpose of his business with you. But when your customer is a company, conducting CDD on the company alone is not enough to prevent financial crime. You need to understand the people who ultimately control the company and benefit from its actions. Illicit actors commonly attempt to hide their identities by conducting business through companies they control.
The individuals who ultimately own and control a company are known as its "beneficial owners." Under Qatari Law, you are required to identify and conduct CDD on every beneficial owner who owns at least 20% of the company you're dealing with, or controls at least 20% of the voting rights. If no one meets that description, then you're required to identify and conduct CDD on every individual who controls the company in other ways. And if you still can't identify anyone who meets that description, you're required to identify and conduct CDD on the company's senior managing official. You are prohibited from carrying out a cash transaction above 50,000 QR with a company unless you have identified and conducted CDD on at least one individual who meets at least one of these definitions!
Example: You agree to sell QR 100,000 in gold bullion to a foreign import export firm, Pearl Enterprises. The customer wishes to pay in cash. You are required to identify and conduct CDD on all individuals in red below.



As a general rule, you are not legally required to identify and conduct CDD on B.H, because he only owns 12 % of your customer, Pearl Enterprises. But if you have any concerns or suspicions (for instance, if you think that he actually fully controls Oyster LLC, despite only owning 20% of it), then you must conduct CDD on him anyway.

You must feel comfortable that you fully understand your customer and the purpose of the transaction. If you do not, and you proceed with the transaction anyway, you could be liable to prosecution even if you complied with the basic requirements of the law and the MOCI Rules.

7- Politically Exposed Persons (PEPs)

PEPs are considered as a high-risk category of customers in relation to Money Laundering (ML). Due to their influence and prominent functions entrusted to them by Qatar or by a foreign State or by an international organization, it is recognised that PEPs are in positions that they can abuse or misuse for their personal gain; or that allow them to misuse or misappropriate Public Funds. PEPs often rely on their family members or close associates to conceal funds accruing from the misuse of their public functions. Therefore, under Qatari law you are required to treat the family members and close associates of PEPs as if they themselves were PEPs.

I. Who are the PEPs?

1. PEPs are individuals who have been entrusted by Qatar or by a foreign State with prominent public functions, such as Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned companies, members of Parliaments, and important political party officials, and members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions in international organizations.

2. Family members of a Politically Exposed Person shall include any natural person relative by blood or marriage up to the second degree; who are: Father/ Mother, Husband/Wife, Father-in-Law/ Mother-in Law, Son/Daughter, Stepson/Stepdaughter, Grandfather/Grandmother, Brother/Sister, Brother-in Law/ Sister –in- Law, Grandson/Granddaughter.

3. Close associates of a Politically Exposed Person: shall include any natural person who is a partner in a legal person or legal arrangement, or a beneficial owner of a legal person or arrangement owned or effectively controlled by a politically exposed person, or any person associated with the politically exposed person through a close business or social relationship.

II. What are the measures that the Dealers in Precious Metals or Precious Stones must adopt when the customer or the customer's beneficial owner is a PEP or a PEP's family member or a close associate?

DPMS are required to put in place appropriate risk management systems to determine whether a customer or a customer's beneficial owner is a PEP, a family member or a close associate of a PEP. The risk management system must include, in particular, seeking relevant information from customers, reference to publicly available information and having access to databases within the limits provided by the applicable legislations.

In this case, DPMS must adopt further CDD measures, as follows:

- Obtain Senior Management approval before establishing a business relationship with a PEP, their family members, or close associates, or continuing a business relationship for existing customers who are PEPs, their family members, or close associates (In cases where DPMS exercise activities as part of a commercial company);

- Take reasonable measures to establish the source of wealth and funds of customers and beneficial owners of customers identified as PEPs, their family members or close associates;

- Conduct enhanced ongoing monitoring on business relationships with PEPs, their family members, and close associates, in addition to ongoing monitoring of transactions conducted within the business relationship while ensuring its consistency with customer's activity pattern and the risks it represents.

8- Record Keeping:

I. What records, Dealers in Precious Metals or Precious Stones should keep?

DPMS should keep:

1. Records, documents and data on all domestic and international transactions and operations.

2. Records, documents and data obtained or collected while performing CDD.

3. Account files, business correspondence, and results of any analysis undertaken

4. All relevant information that enables tracing all financial transactions, when performing cash transactions or attempted transactions by the customer, and all related reports.

- ### II. How long records must be kept?

1. Pursuant to the requirements set forth in Article (20) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing, DPMS shall maintain all records, documents and data for all domestic and international transactions and operations, for a minimum of ten (10) years:

(1) From the date of concluding the transaction, domestic or international occasional transaction or operation.
(2) Following the termination of the business relationship

2. DPMS must retain records beyond the end of the ten-year period mentioned above:

1) If they have filed with the QFIU a suspicious transaction report relating to the applicant for business or customer.
2) If they know that the applicant for business or customer is under investigation by law enforcement or judicial authorities for issues related to money laundering or terrorism financing.

III. To whom should Dealers in Precious Metals or Precious Stones make records available?

DPMS should ensure that all CDD records, data and documents on transactions and operations are available without delay to the competent authorities upon request.
DPMS should also establish proper systems to ensure prompt response to the requests of the competent authorities.

1. IV: What is the purpose of keeping records?

1.They provide proof of compliance with AML/CFT requirements.

2.They allow authorities to reconstruct individual transactions so as to provide, if necessary, evidence for the prosecution of criminal activity.

3.They allow the Dealer to respond to requests by QFIU, supervisory authorities, competent authorities, law enforcement authorities or judicial authorities.

9- Reporting Suspicious Transactions

DPMS must report promptly to QFIU any suspicious financial transaction or any attempt to perform such transactions, regardless of the amount of the transaction, when they suspect or have reasonable ground to suspect that:

a) the transactions are linked to or include funds that are proceeds of a predicate offence;

b) or are linked to terrorism financing.

DPMS should comply with the reporting obligations, when they suspect or have reasonable grounds to suspect that the transactions are linked to or involve proceeds of a predicate offence, or relating to terrorism financing, irrespective of the following:

- the amount of the transaction;
- No transaction has been conducted;
- The nature of the predicate offence
- Any attempt of money laundering or terrorism financing has failed.

The reporting obligation does not require the reporting entity to provide accurate evidence or supporting information in relation to the committed predicate offence or the need to provide the accurate legal description thereof.

"Reasonable grounds to suspect" is determined by what is reasonable in the Dealers in Precious Metals or Precious Stones' circumstances, including normal business practices and systems within the industry.

Annex 4 of this document contains a list of indicators of suspicious transactions regarding DPMS, as specified by the QFIU. This list of indicators is not an exclusive list. They can identify suspicious transactions involving high-risk individuals, legal entities, and transactions based on other criteria or known indicators of money laundering, terrorist financing, or a predicate offence.

What Kind of Transactions Must You Report?

Under Law (20) of 2019, DPMS are only required to report a suspicious transaction when the underlying transaction, or attempted transaction:

- Is conducted in cash; and
- The total value of the transaction (including any linked transactions), is equal to or greater than QR 50,000.

DPMS are not prohibited from reporting suspicions related to other types of transactions, however—such as cash transactions under QR 50,000 and credit card transactions. They are encouraged to do so if they believe that their may be a link to money laundering or terrorist financing.

A. How to Identify a Suspicious Transaction?

Transactions, whether completed or attempted, may give rise to reasonable grounds to suspect that they are related to money laundering or terrorist financing regardless of the sum of money involved. There is no monetary threshold for making a report on a suspicious transaction. A suspicious transaction may involve several factors that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist financing offence, or both.

As a general guide, a transaction may be connected to money laundering or terrorist financing when the transaction (or a series of transactions) raises questions or gives rise to discomfort, apprehension, or mistrust. The context in which the transaction or transactions occur or are attempted is a significant factor in assessing suspicion. This will vary from business to business, and from one Customer to another.

Reporting DNFBPs should evaluate transactions using a risk-based approach, in an appropriate manner, within the normal practices in their particular line of business, and based on their knowledge of their customer. Transactions that are inconsistent with the customer profile established at onboarding or that do not appear to be in keeping with normal industry practices may be relevant factors for determining whether there are reasonable grounds to suspect that the transactions are related to money laundering or terrorist financing.

An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behaviour. Remember that behaviour is suspicious, not people. Suspicion could be based on a single factor, or it could be based on the combination of a number of factors. All circumstances surrounding a transaction or series of transactions should be reviewed.

DPMS, in determining whether or not the occasional transaction or inconsistent transaction is suspicious, should consider:

a. whether the transaction has no apparent or visible economic or lawful purpose;

b. Whether the transaction has no reasonable explanation;

c. Whether the size or pattern of the transaction is not similar to the earlier size or pattern of the transactions of the same or similar customers;

d. Whether the customer has failed to provide an adequate explanation or full information on the transaction.

e. Whether the transaction involves a newly established business relationship, or is a one-off transaction.

f. Whether the transaction involves offshore accounts, companies, or structures that are not supported by the customer's economic needs.

g.Whether the transaction involves unnecessary routing of funds through third parties.

B. Who submits the STR?

The STR should be made by the compliance officer or his Deputy. DPMS shall provide QFIU with the contact information of their compliance officers or deputy compliance officers and shall update QFIU of any changes thereto.

C. When to submit the STR?

1. DPMS shall promptly submit a STR to report any suspicious transaction or operation or on any attempt to perform such transaction or operation, irrespective of its value, when suspecting or having reasonable grounds to suspect that it is the proceeds of a predicate offence or in relation to terrorism financing, **within three (3) business days** from the day of identifying the transaction as suspicious.

2. When there is suspicion that the transactions are linked to, or to be used in terrorist acts or by terrorist organizations, the STR must be submitted **within twenty-four (24) hours from the date of determining that the transactions were suspicious or having reasonable grounds to believe that the transactions are linked to a criminal activity.**

3. For attempted transactions, when DPMS receive an order from a customer to execute a transaction, and the said Dealers suspect that the transaction's proceeds are from a criminal activity and/or are related to money laundering, or are linked to, or to be used in terrorist acts or by terrorist organizations, the STR must be submitted within twenty four (24) hours from the date of determining that the transactions were suspicious, or on the first business day, whichever is soonest.

Non-business days are excluded from the counting of the prescribed reporting period. The following are considered non-business days:
a. Weekend (Friday and Saturday).

b. Official national holiday.

c. Officially declared national holiday (Special non-business day nationwide).

4. DPMS should notify the Anti-Money Laundering and Terrorism Financing Section of the STR submitted to the QFIU for supervisory and statistical purposes without providing details about the content of that report.

D. How to submit STRs?

DPMS must submit STRs through the QFIU Electronic STR System (E-STR). The QFIU is currently preparing to allow DPMS to submit STRs electronically. They will be notified when that system is availabale.

If E-STR is not available, the STR shall be submitted by driver/courier to the QFIU Office as follows:

Qatar's National Financial Crime Centre,

Building 11, 8th Floor

Al Baladiya Street 810, Doha - Qatar

P.O. Box 1234

E. Report contents

DPMS shall submit STRs to the QFIU and complete all relevant fields in the standard form with as much accurate information as is available in the Suspicious Transaction Report Form adopted by the QFIU and the instructions issued by the QFIU, as enclosed herewith.

STRs are filed on a "suspect" basis. The suspect may be a customer or a non-customer. DPMS shall indicate in the narrative field of the STR on the number of suspicious transactions, provide the transaction details separately as an Excel file and then submit it to the QFIU as a STR attachment.

DPMS should disclose in any subsequent STR involving the same suspect that the suspicious transaction is related to another STR distinct from the previous one, by including the reference number of the suspicious transaction in the STR.

F. Reporting obligations

1. DPMS are protected from both criminal and civil liability for breach of any restriction on disclosure of information imposed by law or regulation or by administrative order or contract, if they report their suspicions in good faith; even if they did not know what the underlying predicate offence was, and regardless of whether the offence actually occurred.

2. DPMS shall be prohibited from disclosing to any unauthorized person whether or not a suspicious transaction report, or any other relevant information is being filed with the QFIU (tipping off). Failure to comply with this requirement shall result in imposing the sanctions stipulated in Article (84) of the AML/CFT Law[15] .

3. DPMS may share information on STRs with foreign branches and majority-owned associates to the extent that this is necessary to maintain a unified AML/CFT program.

15- Article (84) of the AML/CFT Law stipulates that: « Any person who commits the offence of disclosing information that may reveal that a suspicious transaction report has been submitted to the Unit, or has not been submitted, shall be sentenced to imprisonment for a term not exceeding three (3) years and a fine not more than (QR 500.000) five hundred thousand Qatari Riyals, or one of these two penalties ».

G. Requests for Information by the QFIU

Pursuant to Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing, the QFIU may request information that is deemed necessary for the performance of its duties. The QFIU may request information from any person or entity subject to reporting obligations. The requested information shall be submitted within the timeframe and form specified by the Unit.

Reporting Entities, including Dealers in Precious Metals or Precious Stones, shall comply with requests for information submitted by the QFIU with regard to suspicious transactions or information that may be associated with money laundering and terrorism financing.

H. Non-compliance and Tipping-Off

Reporting entities are required to comply with the requests for information received from the QFIU with regard to suspicious transactions or transactions associated with money laundering and terrorism financing.

In case of non-compliance by a reporting entity, or non-response to the QFIU requests, the QFIU shall adopt the following procedures:

1. following the lapse of the timeframe specified in this Guidance to submit a report or the deadline set to comply with the request, the QFIU shall issue a reminder to comply with the requirements of the reporting or request within three (3) days;

2. After the lapse of the grace period, the QFIU shall warn the DPMS that their continued non-compliance will be reported to their supervisory authority. They shall be given another three (3) days to comply.

3. With the continued non-compliance by DPMS, the QFIU shall inform the relevant AML/CFT Section of their non-compliance to take the necessary administrative and financial measures and penalties.

Reporting Entities that fail to meet their obligations under Law No. (20) of 2019 could be subject to financial and administrative measures and penalties.

Chapter Two: Sanctions and Penalties Imposed on Dealers in Precious Metals or Precious Stones for Breach of AML/CFT Obligations

In the event of a breach to the AML/CFT obligations, Dealers in Precious Metals or Precious Stones will be subject to the sanctions and penalties provided for in the law regulating the combating of money laundering and terrorism financing.

1. Penalities:

Article (82) of Law No. (20) on Combating Money Laundering and Terrorism Financing stipulates that directors, board members, owners, authorized representatives or any other employees of financial institutions and DNFBPs shall be sentenced to imprisonment for a term not exceeding two (2) years or a fine not less than (QR 5.000.000) five million Qatari Riyals and not more than (QR 10.000.000) ten million Qatari Riyals, or one of these two penalties, when contravening, whether wilfully or as the result of gross negligence, the provisions stipulated in the following Articles of the same law:

(9) : keeping anonymous accounts or accounts in obviously fictitious names

(10): failure to undertake Customer Due Diligence measures in cases determined by the Law.

(11): failure to undertake measures to identify customers, whether permanent or occasional / initiate or maintain a business relationship or carry out any transaction when they are unable to comply with these measures or when they discover that the customers' data obtained is obviously fictitious or inadequate.

(13): failure to apply EDD measures in cases determined by the Law.

(14): failure to keep data and information related to the CDD processes up-to-date and relevant on an ongoing basis.

(15): failure to perform CDD measures proportionate to the level of risks involving the customers, their businesses and their transactions.

(16): failure to put in place appropriate risk management systems to determine whether a customer or beneficial owner of a customer is a Politically Exposed Person (PEP), a family member of a PEP, or a close associate of a PEP/ Failure to take additional relevant measure if the above is determined.

(20): failure to maintain records / failure to make all information available to authorities upon request.

(21): failure to promptly report to the QFIU any information concerning any transaction or operation, including attempted transactions and operations, regardless of the value thereof, when there is a suspicion or reasonable grounds to suspect that such transactions and operations are associated with, or involve proceeds of a predicate offence or may be used in terrorism financing.

2. Financial and Administrative sanctions:

Article (44) of Law No. (20) on Combating Money Laundering and Terrorism Financing stipulates that without prejudice to a more severe penalty stipulated in any other law, and in case it is evidenced that any DNFBP, or any of the directors, board members, executives or management thereof, has violated the provisions of this Law, its Implementing Regulations and any decisions or guidance related to AML/CTF, the AML/CFT Section may impose one or more of the following measures:

1. Sending written warnings.

2. Ordering regular reports on the measures taken.

3. Ordering compliance with specific instructions.

4. Imposing a financial penalty of no less than (QR 25.000) twenty-five thousand Qatari Riyals, and no more than (QR 100.000) one hundred thousand Qatari Riyals per violation per day, on the DNFBP after being notified.

5. Imposing a financial penalty of no more than (QR 100.000.000) one hundred million Qatari Riyals on the violating DNFBP.

6. Imposing a financial penalty of no more than (QR1.000.000) one million Qatari Riyals on any of the directors, board members, executives or management.

7. Restricting the powers of the directors, board members, executives, or management, in addition to appointing a special administrative supervisor, or subjecting the DNFBP to direct control.

8. Prohibiting the perpetrator from working in the relevant sectors, either temporarily or permanently.

9. Suspending, dismissing or replacing directors, board members, executives, management, trustees of trusts, or trustees, either temporarily or permanently.

10. Imposing suspension of the license, restricting any other type of permit, and prohibiting the continuation of work, the profession or the activity, or barring the name from the relevant registry.

11. Revoking and withdrawing licenses and registrations.

The decisions referred to may be appealed in accordance with the controls, procedures and timelines set forth in articles 64 and 65 of the Implementing Regulation of the AML/CFT Law.

• International References

- FATF REPORT/ Money laundering/Terrorist financing risks and vulnerabilities associated with gold,July 2015.

- MENAFATF-DNFBPs in relation to AML/CFT, 10November 2008.

- RBA Guidance for Dealers in Precious Metals and Stones,FATF,17 June 2008,p23.

• Legal References

1. Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing.

2. Law No. (1) of 2020 on the Unified Economic Register.

3. Council of Ministers' Decision No. [41] of 2019 Promulgating the Implementing Regulations of Law No. (20) of 2019 on Combatting Money Laundering and Terrorism Financing.

4. Council of Ministers' Decision No. [12] of 2020 Promulgating the Implementing Regulations of Law No. (1) of 2020 on the Unified Economic Register.

5. Decision of the Minister of Commerce and Industry No. (95) of 2019 on establishing the Anti-Money Laundering and Terrorism Financing Section under the Companies Affairs Department.

6. Decision of the Minister of Commerce and Industry No. (48) of 2020 promulgating AML/CFT Rules for legal Auditors, Dealers in Precious Metals or Precious Stones and Trusts and Company Service Providers.

• Useful links

1. Financial Action Task Force (FATF)
https://www.fatf-gafi.org/

2. Middle East and North Africa Financial Action Task Force on Combating money laundering and financing of terrorism (MENAFATF)
http://www.menafatf.org/

3. National Anti-Money Laundering & Terrorism Financing Committee
http://www.namlc.gov.qa/

4. Qatar Financial Information Unit
http://www.qfiu.gov.qa/

5. Anti-Money Laundering and Terrorism Financing Section at the Minstry of commerce and Industry
https://www.moci.gov.qa/مكافحة-غسل-الأموال-و-تمويل-الإرهاب/

mail address: control.aml@moci.gov.qa
Address: 2 floor Ministry of Commerce and Industry Lusail City, Qatar

Annexes

Annex 1: circular No. (6) of 2020 for Auditors, Dealers in Precious Metals and Stones and Trust and Company Service Providers about High-Risk Jurisdictions Subject to A Call for Action by the Financial Action Task Force and Jurisdictions Under Increased Monitoring

وزارة التجارة والصناعة

Ministry of Commerce and Industry

Companies Affairs Department — إدارة شؤون الشركات

Circular No. (6) of 2020 for Auditors, Dealers in Precious Metals and Stones and Trust and Company Service Providers about High-Risk Jurisdictions Subject to A Call for Action by the Financial Action Task Force and Jurisdictions Under Increased Monitoring

Gentlemen / Auditors, Dealers in Precious Metals and Stones and Trust and Company Service Providers,

Pursuant to the requirements of Article (13) of Law No. (20) of 2019 issuing the Anti-Money Laundering and Terrorist Financing Law,

And Articles (22), (23) and (60) of the executive regulations of the Anti-Money Laundering and Terrorist Financing Law issued by Cabinet Resolution No. (41) of 2019,

And Article (2) of the Decision of Minister of Commerce and Industry No. (95) of 2019 establishing the Anti-Money Laundering and Terrorist Financing Section in the Companies Affairs Department,

The Anti-Money Laundering and Terrorist Financing Division issues the following circular:

The Financial Action Task Force (FATF) identifies, three times per year and in a public statement, jurisdictions whose regimes have strategic deficiencies in terms of combating money laundering, terrorism financing and the financing of proliferation of weapons of mass destruction, in which it calls upon countries to adopt certain measures against them. In accordance with its latest meeting in February 2020, FATF issued a statement regarding the list of those jurisdictions and the measures and procedures that must be adopted.

In light of such event, the National Anti-Money Laundering and Terrorism Financing Committee (NAMLC) published on its website (www.namlc.gov.qa) the link to FATF's statement and issued letter No. 1417/2020 dated 13/04/2020 in which it called upon supervisory authorities to require their supervised entities to adopt due diligence measures when dealing with the jurisdictions concerned, implement procedures and instructions relevant to combating money laundering and terrorism financing and related to dealing with high-risk jurisdictions and other jurisdictions under monitoring, based on FATF's requirements

indicated above and Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing and its Implementing Regulations.

Jurisdictions whose regimes have strategic deficiencies in combating money laundering and terrorism financing are distributed as follows:

a- **High-risk jurisdictions subject to a call for action by FATF:**

High-risk jurisdictions have significant strategic deficiencies in their regimes to counter money laundering, terrorist financing, and financing of proliferation of weapons of mass destruction. For all countries identified as high-risk, the FATF calls on all members to apply enhanced due diligence (EDD), and in the most serious cases, countries are called upon to apply counter-measures to protect the international financial system from the ongoing money laundering, terrorist financing, and financing of proliferation of weapons of mass destruction risks emanating from the country. This list currently includes:

I. **Democratic People's Republic of Korea (DPRK):**

FATF reaffirms in its latest statement its call on its members to advise their financial institutions and designated non-financial businesses and professions (DNFBPs) to give special attention to business relationships and transactions with the DPRK, including DPRK companies, financial institutions, and those acting on their behalf. FATF further calls on its members to continue applying **EDD and counter-measures** and to implement **targeted financial sanctions** in accordance with applicable United Nations Security Council Resolutions.

Accordingly, auditors (chartered accountants), dealers in precious metals and stones and trust and company service providers must undertake the following:

وزارة التجارة والصناعة
Ministry of Commerce and Industry
Companies Affairs Department إدارة شؤون الشركات

1. **Implementing EDD** that is proportionate to the level of risk for business relationships and operations carried out with customers, including financial institutions and DNFBPs from DPRK[1], as follows[2]:
   - Examining, as much as possible and in a reasonable manner, the background and purpose of all complex or unusual operations and all unusual patterns of operations that have no apparent legal or economic purpose.
   - Increasing the level of monitoring for the business relationship to identify unusual or suspicious activities or operations.
   - Obtaining additional information on the nature of the expected business relationship.
   - Obtaining senior management approval to establish or continue the business relationship.
2. **Implementing counter-measures** for business relationships and operations carried out with customers, including financial institutions and DNFBPs from DPRK, as follows[3]:
   - Submitting immediate reports to the AML/CFT Section at the Companies Affairs Department at MOCI on business relationships and operations carried out with that jurisdiction or persons located in it.
3. **Implementing targeted financial sanctions** related to combating terrorism and terrorism financing and preventing proliferation of weapons of mass destruction against DPRK according to the provisions of Law No. (27) of 2019 on Combating Terrorism and Decision No. (1) of 2020 of the Public Prosecutor Regulating the Implementation Mechanisms of the Targeted Financial Sanctions related to Combatting the Financing of Terrorism and the Financing of the Proliferation of Weapons of Mass Destruction pursuant to the Law on Combating Money Laundering

[1] Article (13) of the Law on Combating Money Laundering and Terrorism Financing and Article (22) of its Implementing Regulations.
[2] Article (25) of the Implementing Regulations of the Law on Combating Money Laundering and Terrorism Financing.
[3] Article (13) of the Law on Combating Money Laundering and Terrorism Financing and Article (23) of its Implementing Regulations.

and Terrorism Financing and the Law on Combating Terrorism and the United Nations Security Council Resolutions, in addition to Decision No. (59) of 2020 of the Public Prosecutor issuing the Guidelines to the Effective Implementation of the Targeted Financial Sanctions Regime in the State of Qatar.

II. Iran:

FATF decided to **re-impose counter-measures against Iran** and called upon its members to apply them. This step followed Iran's failure to comply with implementing the action plan related to addressing deficiencies in countering money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in its regime within the period specified. The most significant deficiencies relate to Iran's failure to ratify the United Nations Convention against Transnational Organized Crime (Palermo Convention) and the Terrorist Financing Convention.

Accordingly, auditors (chartered accountants), dealers in precious metals and stones and trust and company service providers must undertake the following:

1. **Implementing EDD** that is proportionate to the level of risk for business relationships and operations carried out with customers, including financial institutions and DNFBPs from Iran[4], as follows[5]:
   - Examining, as much as possible and in a reasonable manner, the background and purpose of all complex or unusual operations and all unusual patterns of operations that have no apparent legal or economic purpose.
   - Increasing the level of monitoring for the business relationship to identify unusual or suspicious activities or operations.
   - Obtaining additional information on the nature of the expected business relationship.

[4] Article (13) of the Law on Combating Money Laundering and Terrorism Financing and Article (22) of its Implementing Regulations.
[5] Article (25) of the Implementing Regulations of the Law on Combating Money Laundering and Terrorism Financing.

وزارة التجارة والصناعة

Ministry of Commerce and Industry

Companies Affairs Department إدارة شؤون الشركات

   - Obtaining senior management approval to establish or continue the business relationship.
2. **Implementing counter-measures** for business relationships and operations carried out with customers, including financial institutions and DNFBPs from Iran, as follows[6]:
   - Implementation of the following EDD for business relationships and operations carried out with customers, including financial institutions and DNFBPs from Iran:
     - Obtaining additional information on the customer, including the profession, size of assets and information available through public databases and open sources, and updating customer and beneficial owner identification data regularly.
     - Obtaining additional information on the nature of the expected business relationship.
     - Obtaining information on the source of the customer's wealth or funds.
     - Obtaining information on the reasons for the expected operations or operations conducted.
     - Applying enhanced monitoring for the business relationship by increasing the extent and period of supervision and selecting patterns of operations that need additional scrutiny and review.
     - Making the first payment through an account in the customer's name in one of the banks subject to similar due diligence standards.
   - Submitting immediate reports to the AML/CFT Section at the Companies Affairs Department at MOCI on business relationships and operations carried out with that jurisdiction or persons located in it.

Auditors (chartered accountants), dealers in precious metals and stones and trust and company service providers must periodically view updates of the list of high-risk jurisdictions subject to a call for action by FATF via the following link:

[6] Article (13) of the Law on Combating Money Laundering and Terrorism Financing and Article (23) of its Implementing Regulations.

http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html

b- Jurisdictions under increased monitoring:

Jurisdictions under increased monitoring are jurisdictions whose regimes have strategic deficiencies in countering money laundering, terrorist financing and financing of proliferation but that have highly complied with FATF's action plan. These jurisdictions are subject to monitoring by FATF until the fulfilment of the action plan within a specific timeframe. FATF does not call upon its members to apply EDD against these jurisdictions; on the other hand, **it urges them, upon analysis of risks related to such jurisdictions, to take into account information published on the link indicated below.**

The list of these jurisdictions under monitoring currently includes: **Albania, The Bahamas, Barbados, Botswana, Cambodia, Ghana, Iceland, Jamaica, Mauritius, Mongolia, Myanmar, Nicaragua, Pakistan, Panama, Syria, Uganda, Yemen and Zimbabwe.**

Accordingly, auditors (chartered accountants), dealers in precious metals and stones and trust and company service providers must undertake the following:

1. Periodically viewing updates of the list of jurisdictions under increased monitoring to take into account, upon analysis of risks, information published on the following link regarding business relationships and operations carried out with customers, including financial institutions and DNFBPs from such jurisdictions[7]:

http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/documents/increased-monitoring-february-2020.html

[7] Article (24) of the Implementing Regulations of the Law on Combating Money Laundering and Terrorism Financing.

Furthermore, in its latest meeting, FATF excluded the Republic of Trinidad and Tobago from the list of jurisdictions under increased monitoring due to its success in implementing the action plan related to addressing deficiencies in countering money laundering, terrorist financing and financing of proliferation of weapons of mass destruction in its regime.

For view and implementation

Salem bin Salim Al Mannai

Director of the Companies Affairs Department

Annex 2: Circular No. (5) of 2020 on Dealers in Precious Metals or Stones in Terms of Implementation of Enhanced Customer Due Diligence for Non-Face-to-Face Transactions.

Gentlemen / Dealers in Precious Metals and Precious Stones,

Pursuant to the requirements of Article (15) of Law No. (20) of 2019 issuing the Anti-Money Laundering and Terrorist Financing Law,

And Articles (25) and (60) of the executive regulations of the Anti-Money Laundering and Terrorist Financing Law issued by Cabinet Resolution No. (41) of 2019,

And Article (2) of the Decision of Minister of Commerce and Industry No. (95) of 2019 establishing the Anti-Money Laundering and Terrorist Financing Section in the Companies Affairs Department,

The Anti-Money Laundering and Terrorist Financing Division issues the following circular:

Within the framework of preventive procedures and precautionary measures taken by the State to limit the spread of the Coronavirus (Covid-19), the Ministry of Commerce and Industry (MOCI) has issued a circular on temporary closure of all shops and commercial and service activities since the beginning of March 2020, including shops that sell precious metals and stones.

It was revealed to MOCI that purchase and sale of precious metals and stones have increased during the period of closure of commercial shops via websites, without taking into account the requirements of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing and its Implementing Regulations that dealers in precious metals and stones must comply with when they conduct transactions in cash or attempt to conduct a transaction with their customers of a value equivalent to or exceeding 50 thousand Qatari Riyals or of equivalent value in other currencies, whether consisting of one or several transactions conducted in a manner that indicates a relation between them.

MOCI also noticed some individuals conducting trade in precious metals or stones through electronic platforms without registration in the Commercial Registry and obtaining a commercial license, which represents a violation of the provisions of Article No. (7) of Law No. (25) of 2005 on the Commercial Register which stipulates the following:" No physical person or legal entity may practice commercial activities or establish a business prior to being registered in the Commercial Register".

Within the scope of supervision conducted by MOCI over the practice of business activities in the State, and as the supervisory authority for dealers in precious metals and stones in the area of combating money laundering and terrorism financing, the following must be complied with:

Firstly: Implementing all requirements needed for the practice of business activities via websites:

MOCI warns of the severity of the practice of trade via websites in the sector of precious metals and stones without following the legal procedures required to conduct business activities and confirms that it will trace violators and notify the Public Prosecution or the competent law enforcement officers in terms of violation of the provisions of Article (16) of Law No. (25) of 2005 indicated above.

Secondly: Implementing all AML/CFT requirements when conducting transactions via websites:

MOCI affirms the need of compliance of dealers in precious metals and stones with AML/CFT requirements stipulated in Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing and its Implementing Regulations, when they conduct transactions in cash with their customers of a value equivalent to or exceeding 50 thousand Qatari Riyals or of equivalent value in other currencies, whether consisting of one or several transactions conducted in a manner that indicates a relation between them via websites, including the adoption of customer due diligence measures to identify regular or occasional customers and the beneficial owner and understand the nature of the customer's business or activity pattern and the nature and purpose of the business relationship, in addition to maintaining all records, documents and data of all local and international transactions and operations for at least 10 years after the date on which the transaction or operation ends.
Given the increase in risks associated with non-face-to-face transactions, including transactions that are conducted through electronic points of sale and that use payment in cash upon delivery of the merchandise or payment cards, the AML/CFT Section in the Companies Affairs Department at MOCI calls upon all dealers in precious metals and stones to implement enhanced due diligence measures for non-face-to-face transactions through the following:

1. Obtaining additional information on the customer, including the profession, size of assets and information available through public databases and open sources.

2. Verifying the identity of the customer included in the non-face-to-face interaction through electronic identification documentation (scanned or photocopied), with the possibility of requesting additional documents to identify the customer.

3. Implementing additional measures to verify the electronic identification documentation, including conducting a direct interview with the customer through a video call (such as Skype or Zoom) to compare physiological characteristics of the customer with scanned or photocopied identity documents, requesting a front-view selfie from the customer that can be compared with electronic identity documents or contacting the customer to ask questions about his identity and the reason for requesting a certain service, as well as other questions that help confirm the identity of the customer.

4. Updating customer and beneficial owner identification data regularly.

5. Applying enhanced monitoring for the business relationship by increasing the extent and period of supervision and selecting patterns of operations that need additional scrutiny and review.

6. Requiring customers involved in the non-face-to-face interaction to make the first payments through accounts in their names at financial institutions subject to similar criteria in terms of due diligence measures.

In case of non-compliance with these requirements, the violator shall be subject to administrative and financial penalties stipulated in Article (44) of Law No. (20) of 2019 on Combating Money Laundering and Terrorism Financing, in addition to imprisonment and fine stipulated in Article (82) of the same Law.

Salem bin Salim Al Mannai
Director of the Companies Affairs Department
Issued on: 01/07/2020

Qatar Financial Information Unit (QFIU)
QFIU Suspicious Transaction Report Form

1.	Submission details:	
1.1	Date:	
1.2	Submitting Officer:	
1.3	Type of Reporting Institution:	☐ Bank ☐ Exchange House ☐ Insurance Company ☐ Investment Company ☐ Finance Company Asset ☐ Management Company ☐ Auditors Lawyers ☐ Real Estate ☐ Brokers/Agents ☐ Dealers in precious metals or precious stones . ☐ Other: (Please specify)
1.4	Submitting Institution:	
1.5	Contact details: Address: Direct Phone No: Email:	
1.6	Your reference No.	

2.	Reporting Details:

2.1	Is this report related to a previously filed STR? (Mandatory	☐ Yes If yes, include the reference number to the report_____ ☐ No
2.2	Is this report related to Terrorism Financing, Money Laundering, Sanctions or other type of suspicion? (Mandatory)	☐ Terrorism Financing ☐ Money Laundering ☐ Sanctions ☐ Another type of Suspicion ☐ Other
2.3	Is this report subject to any urgent requirements to freeze funds?	☐ Yes ☐ No ☐ Unknown
2.4	Reason for suspicion (Mandatory)	☐ Structuring ☐ Unusual transaction ☐ Source of funds not established ☐ Uneconomical transaction ☐ Transaction with no business purpose ☐ Fraud ☐ Incomplete KYC ☐ False identity ☐ Large amount of cash ☐ Conduct of the individual suspicious ☐ Other : (Please Specify)
2.5	Number of transactions reported (Mandatory)	☐ One transaction ☐ Multiple transactions ○ No. of Transactions

2.6	Number of transactions reported (Mandatory)	Value in Qatari Riyal: Value in other Currencies:
2.7	What type of fund, service or product was used for the transaction? (Mandatory)	☐ Cash ☐ Wire transfer ☐ Bank account ☐ Trust Account ☐ Securities ☐ Cheque ☐ Insurance policy ☐ Investment Certificates ☐ Stocks ☐ Currency Exchange ☐ Credit Card ☐ Debit Card ☐ Crypto Currency ☐ Gold ☐ Other precious metal ☐ Diamonds ☐ Other precious stones ☐ Real estate ☐ Consulting/ Advisory services ☐ Other: (Please specify)

3.	Details of the person/s of interest (POI)/ Suspect or associates related to the transaction Details of the person/s of interest (POI)/ Suspect or associates related to the transaction If the POI is a natural person fill Part 3, If POI/ Suspect is a legal person fill Part 5. If the POI / Suspect involves both natural and legal persons fill both Part 3 and 5. If POI/ Suspect is a Trust, fill Part 6.	
3.1	**Person of Interest:** Provide as many details as you know about the POI/ Suspect and include copies of any identification documents obtained	○ Nationality and Residency Information ○ Nationality:(Mandatory) ○ **Qatari:** ☐ QID No.(Mandatory) ☐ Passport No. (Optional) ○ **Resident** ☐ QID No. (Mandatory) ☐ Passport No. (Optional) ○ **GCC Countries (Either/or)** ☐ QID No. ☐ Passport No ○ **Non Resident** ☐ Passport No. (Mandatory) ☐ Name in Arabic: ☐ Name in English: ☐ (Either Arabic or English Name Mandatory) ☐ Date of birth (Mandatory): ☐ Gender (Mandatory): ☐ Address/s: ☐ Phone Number: ☐ Mobile Number: ☐ Email Address: ☐ Country of Residence: ☐ Occupation: ☐ Driver's license details: ☐ Employer details: ☐ Any other personal information:

4.	Account Information (1)	
4.1.1	Account type: (Mandatory)	☐ Retail ☐ Corporate ☐ Other: Details:
4.1.2	Sub-account type:	☐ Personal account ☐ Business account ☐ Trust account ☐ Other: Details:
4.1.3	Account Institution Branch: (Mandatory)	
4.1.4	Account name: (Mandatory)	
4.1.5	Account opening date:	
4.1.6	Account number: (Mandatory)	
4.1.7	Account Signatories:	
4.1.8	Account closed date, if applicable:	
4.1.9	Account balance: (Mandatory)	
4.1.10	Account transaction history:	**Please attach account transaction history covering the period of suspicion**

	Account information (2)	
4-2-1	Account type: (Mandatory)	☐ Retail ☐ Corporate ☐ Other: Details:
4-2-2	Sub-account type:	☐ Personal account ☐ Business account ☐ Trust account ☐ Other: Details:
4-2-3	Account Institution Branch: (Mandatory)	
4-2-4	Account name: (Mandatory)	
4-2-5	Account opening date:	
4-2-6	Account number: (Mandatory)	
4-2-7	Account Signatories:	
4-2-8	Account closed date, if applicable:	
4-2-9	Account balance: (Mandatory)	
4-2-10	Account transaction history:	**Please attach account transaction history covering the period of suspicion**

5. Company/Business Information		
5-1	Name of company/ business: (Mandatory)	
5-2	Type of company/ business: (Mandatory)	☐ Private Company ☐ Public Company ☐ Partnership ☐ Other
5-3	Which jurisdiction is the company / business registered? (Mandatory)	☐ Qatar ☐ Other: Please specify
5-4	Company or Business Registration No. : (Mandatory)	No
5-5	Establishment Code (Mandatory if company / business is local)	No
5-6	Foreign Company Registration No .Mandatory if company / business is foreign)	No
5-7	Registered address: (Mandatory)	
5-8	Operational address, if different from registered address:	
5-9	Company / business contact details:	☐ Name: ☐ Phone No.: ☐ Mobile No.: ☐ Email address: ☐ Other information
5-10	Company Directors and/or business owners.	☐ Name: ☐ Phone No.: ☐ Mobile No.: ☐ Email address: ☐ Other information:
5-11	Reason for association to other person of interest (POI)/ Suspect	

6. Trust		
6-1	Trust name	
6-2	Nature and purpose of the trust	
6-3	Jurisdiction and date of the establishment of the trust	
6-4	Identity of settlor (s)	
6-5	Identity of trustee (s)	
6-6	Identity of protector (s)	
6-7	Beneficiary or beneficiaries	
6-8	Other particulars	

7.	Details of the suspicious activity	
7-1	When did this suspicious activity occur? (Mandatory)	Date/s:
7-2	Where did this suspicious activity occur? (Mandatory)	

7-3	How was the suspicious activity identified? (Mandatory)	☐ Face to face transaction ☐ Transaction monitoring system ☐ Compliance Officer or MLRO ☐ Anonymous Tip ☐ Manual Audit ☐ Negative News ☐ Other (Please specify)
7-4	Provide a detailed narrative about the actual suspicious activity resulting in the filling of this STR. **What raised your suspicions?** Describe clearly and completely the factors or unusual circumstances that led to the suspicion of ML or TF activity. (Mandatory)	
7-5	Provide any additional information that you consider important to filing this STR.	

8.	**Supporting documentation**	
1.8	Please list any supporting documents relevant to the filing of this STR	**List attachments:** ☐ POI/ Suspect Identification documents ☐ Account information ☐ Transaction records ☐ Company/business records ☐ Any other documents or records List:

Annex 4: Indicators of Suspicious Transactions

The following indicators are provided to help assess whether or not transactions might give rise to reasonable grounds for suspicion. These are examples of common indicators that may be helpful when evaluating transactions, whether completed or attempted. These include indicators based on certain characteristics that have been linked to money laundering or terrorist activities in the past.
These indicators are not intended to cover every possible situation and are not to be viewed in isolation. A single indicator is not necessarily indicative of reasonable grounds to suspect money laundering or terrorist financing activity. However, if a number of indicators are present during a transaction or a series of transactions, Reporting Entities might want to take a closer look at other factors prior to making the determination as to whether the transaction must be reported.

The indicators have to be assessed in the context in which the transaction occurs or is attempted. Each indicator may contribute to a conclusion that there are reasonable grounds to suspect that the transaction is related to the commission or attempted commission of a money laundering or a terrorist financing offence. However, it may also offer no indication of this in light of factors such as the client's occupation, business, financial history and past investment pattern. Taken together, the presence of one or more indicators as well as the Reporting Entities' knowledge of its client›s business or financial affairs will help them identify suspicious transactions.

I. Indicators for all reporting entities:

1) General Indicators

- Customer admits or makes statements about involvement in criminal activities.
- Customer does not want correspondence sent to home address.
- Customer appears to have accounts with several financial institutions in one area for no apparent reason.
- Customer conducts transactions at different physical locations in an apparent attempt to avoid detection.
- Customer repeatedly uses an address but frequently changes the names involved.
- Customer is accompanied and watched.
- Customer shows uncommon curiosity about internal systems, controls and policies.
- Customer has only vague knowledge of the amount of a deposit.
- Customer presents confusing details about the transaction or knows few details about its purpose.
- Customer appears to informally record large volume transactions, using unconventional bookkeeping methods or "off-the-record" books.
- Customer over justifies or explains the transaction.
- Customer is secretive and reluctant to meet in person.
- Customer is nervous, not in keeping with the transaction.

- Customer is involved in transactions that are suspicious but seems blind to being involved in money laundering activities.
- Client›s home or business telephone number has been disconnected or there is no such number when an attempt is made to contact Customer shortly after opening account.
- Normal attempts to verify the background of a new or prospective Customer are difficult.
- Customer appears to be acting on behalf of a third party, but does not tell you.
- Customer is involved in activity out-of-keeping for that individual or business.
- Customer insists that a transaction be done quickly.
- Inconsistencies appear in the client›s presentation of the transaction.
- The transaction does not appear to make sense or is out of keeping with usual or expected activity for the client.
- Customer appears to have recently established a series of new relationships with different financial entities.
- Customer attempts to develop close rapport with staff.
- Customer uses aliases and a variety of similar but different addresses.
- Customer spells his or her name differently from one transaction to another.
- Customer uses a post office box or General Delivery address, or other type of mail drop address, instead of a street address when this is not the norm for that area.
- Customer provides false information or information that you believe is unreliable.
- Customer offers you money, gratuities or unusual favours for the provision of services that may appear unusual or suspicious.
- Customer pays for services or products using financial instruments, such as money orders or traveller's cheques, without relevant entries on the face of the instrument or with unusual symbols, stamps or notes.
- You are aware that a Customer is the subject of a money laundering or terrorist financing investigation.
- You are aware or you become aware, from a reliable source (that can include media or other open sources), that a customer is suspected of being involved in illegal activity.
- A new or prospective customer is known to you as having a questionable legal reputation or criminal background.
- Transaction involves a suspected shell entity (that is, a corporation that has no assets, operations or other reason to exist).

2) Knowledge of reporting or record keeping requirement

- Customer attempts to persuade employee not to complete any documentation required for the transaction.
- Customer makes inquiries that would indicate a desire to avoid reporting.
- Customer has unusual knowledge of the law in relation to suspicious transaction reporting.
- Customer seems very conversant with money laundering or terrorist activity financing issues.
- Customer is quick to volunteer that funds are "clean" or "not being laundered."
- Customer appears to be structuring amounts to avoid record keeping, Customer identification or reporting thresholds.

- Customer appears to be collaborating with others to avoid record keeping, customer identification or reporting thresholds.

3) Identity Documents

- Customer provides doubtful or vague information.
- Customer produces seemingly false identification or identification that appears to be counterfeited, altered or inaccurate.
- Customer refuses to produce personal identification documents.
- Customer only submits copies of personal identification documents.
- Customer wants to establish identity using something other than his or her personal identification documents.
- Customer's supporting documentation lacks important details such as a phone number.
- Customer inordinately delays presenting corporate documents.
- All identification presented is foreign or cannot be checked for some reason.
- All identification documents presented appear new or have recent issue dates.
- Customer presents different identification documents at different times.
- Customer alters the transaction after being asked for identity documents.
- Customer presents different identification documents each time a transaction is conducted.

4) Cash transactions

- Customer starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the Customer in the past.
- Customer frequently exchanges small bills for large ones.
- Customer uses notes in denominations that are unusual for the client, when the norm in that business is different.
- Customer presents notes that are packed or wrapped in a way that is uncommon for the client.
- Customer deposits musty or extremely dirty bills.
- Customer makes cash transactions of consistently rounded-off large amounts.
- Customer consistently makes cash transactions that are just under the reporting threshold amount in an apparent attempt to avoid the reporting threshold.
- Customer consistently makes cash transactions that are significantly below the reporting threshold amount in an apparent attempt to avoid triggering the identification and reporting requirements.
- Customer presents uncounted funds for a transaction. Upon counting, the Customer reduces the transaction to an amount just below that which could trigger reporting requirements.
- Customer conducts a transaction for an amount that is unusual compared to amounts of past transactions.
- Customer frequently purchases traveller's cheques, foreign currency drafts or other negotiable instruments with cash when this appears to be outside of normal activity for the client.
- Customer asks you to hold or transmit large sums of money or other assets when this type of activity is unusual for the client.
- Shared address for individuals involved in cash transactions, particularly when the address is also for a business location, or does not seem to correspond to the stated occupation (i.e., student, unemployed, self-employed, etc.)

• Stated occupation of the customer is not in keeping with the level or type of activity (for example a student or an unemployed individual makes daily maximum cash withdrawals at multiple locations over a wide geographic area).

• Cash is transported by a cash courier.

• Large transactions using a variety of denominations.

5) Economic purpose

• Transaction seems to be inconsistent with the client's apparent financial standing or usual pattern of activities.

• Transaction appears to be out of the normal course for industry practice or does not appear to be economically viable for the customer.

• Transaction is unnecessarily complex for its stated purpose.

• Activity is inconsistent with what would be expected from the declared business.

• A business customer refuses to provide information to qualify for a business discount.

• No business explanation for the size of transactions or cash volumes.

• Transactions of financial connections between businesses that are not usually connected (for example, a food importer dealing with an automobile parts exporter).

• Transaction involves non-profit or charitable organization for which there appears to be no logical economic purpose or where there appears to be no link between the stated activity of the organization and the other parties in the transaction.

6) Transactions involving accounts

• Funds are being deposited into several accounts, consolidated into one and transferred outside the country.

• Reactivated dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by frequent cash withdrawals until the transferred sum has been removed.

• Attempting to open or operating accounts under a false name.

• Customer frequently uses many deposit locations outside of the home branch location.

• Opening accounts when the client's address is outside the local service area.

• Opening accounts in other people's names.

• Opening accounts with names very close to other established business entities.

• Account with a large number of small cash deposits and a small number of large cash withdrawals.

• Multiple transactions are carried out on the same day at the same branch but with an apparent attempt to use different tellers.

• Activity far exceeds activity projected at the time of opening the account.

• Establishment of multiple accounts, some of which appear to remain dormant for extended periods.

• Account that was reactivated from inactive or dormant status suddenly sees significant activity.

• Unexplained transfers between the client's products and accounts.

• Large transfers from one account to other accounts that appear to be pooling money from different sources.

• Multiple deposits are made to a client's account by third parties. •

• Frequent deposits of bearer instruments (for example, cheques, money orders or bearer bonds).

• Unusually large cash deposits by a Customer with personal or business links to an area associated with drug trafficking.

• Regular return of cheques for insufficient funds.

• Correspondent accounts being used as "pass-through" points from foreign jurisdictions with subsequent outgoing funds to another foreign jurisdictions.

• Multiple personal and business accounts are used to collect and then funnel funds to a small number of foreign beneficiaries, particularly when they are in locations of concern, such as countries known or suspected to facilitate money laundering activities.

The Financial Action Task Force›s website (http://www.fatf-gafi.org) has information about non-cooperative countries and territories in the fight against money laundering and terrorist financing (see «High-risk and non-cooperative jurisdictions» section).

7) Transactions involving areas outside Qatar

• Customer and other parties to the transaction have no apparent ties to Qatar.

• Transaction crosses many international lines.

• Use of a credit card issued by a foreign bank that does not operate in Qatar by a Customer that does not live or work in the country of issue.

• Cash volumes and international remittances in excess of average income for migrant worker clients.

• Transactions involving high-volume international transfers to third party accounts in countries that are not usual remittance corridors.

• Transaction involves a country known for highly secretive banking and corporate law.

• Transactions involving any countries deemed by the Financial Action Task Force as requiring enhanced surveillance.

• Foreign currency exchanges that are associated with subsequent wire transfers to locations of concern, such as countries known or suspected to facilitate money laundering activities.

• Deposits followed within a short time by wire transfer of funds to or through locations of concern, such as countries known or suspected to facilitate money laundering activities.

• Transaction involves a country where illicit drug production or exporting may be prevalent, or where there is no effective anti-money-laundering system.

• Transaction involves a country known or suspected to facilitate money laundering activities.

The Financial Action Task Force's website (http://www.fatf-gafi.org) has information about non-cooperative countries and territories in the fight against money laundering and terrorist financing (see «High-risk and non-cooperative jurisdictions» section).

8) Transactions related to offshore business activity

- Accumulation of large balances, inconsistent with the known turnover of the client›s business, and subsequent transfers to overseas account(s).
- Frequent requests for traveller's cheques, foreign currency drafts or other negotiable instruments.
- Loans secured by obligations from offshore banks.
- Loans to or from offshore companies.
- Offers of multimillion-dollar deposits from a confidential source to be sent from an offshore bank or somehow guaranteed by an offshore bank.
- Transactions involving an offshore "shell" bank whose name may be very similar to the name of a major legitimate institution.
- Unexplained electronic funds transfer by Customer on an in-and-out basis.
- Use of letter-of-credit and other method of trade financing to move money between countries when such trade is inconsistent with the client's business.
- Use of a credit card issued by an offshore bank.

II. Specific Indicators for DPMS: RED FLAGS[1]

1- Customer behaviour

- Established customer (including bullion dealers) dramatically increasing his purchase of gold bullion for no apparent reason.
- Foreign nationals purchasing gold bullion through multiple transactions over a short time period.
- Bullion transferred among associates using bullion accounts (including family members) for no apparent commercial purpose.
- Occupation inconsistent with customer's financial profile. For example, the customer may list their occupation as 'student' or 'truck driver' yet transfer large values of funds to bullion accounts.
- Customer buying gold bullion and using a General Post Office (GPO), or private service provider, mailbox as their address, without listing a corresponding box number.
- Unusual pattern of bullion transactions and the nature of the transactions are inconsistent with the customer profile.
- A previously unknown customer requester a refiner to turn gold into bullion.

2- Company behaviour

- Non- reporting to the FIU by the gold industry organisations (where there is an obligation to report).

1- FATF REPORT/ Money laundering/Terrorist financing risks and vulnerabilities associated with gold,July 2015. P.6

- Changes to business name of entities registered to deal in gold
- Registration of a trading company in a tax haven even though its business relates to another jurisdiction.
- Movement of abnormally large sums of money in various accounts of the individuals and companies which are not related to the nature of their business.
- Unusual deposits i.e. use of cash or negotiable instruments (such as traveller's cheques, cashier's cheques and money orders) in round denominations (to keep below reporting threshold limit) to fund bank accounts and to pay for gold. The negotiable instruments may be sequentially numbered or purchased at multiple locations and may frequently lack payee information.
- Numerous sole proprietorship businesses/private limited companies set up by seemingly unrelated (proxies) but controlled by the same group of people. False addresses are used to register such businesses.
- Use of corporate structure of shell companies located across the jurisdictions.
- Significant number of companies registered to one natural person
- Commercial activities are not easy to track as the companies are registered elsewhere.
- No clarity of how the company transports the merchandise it has bought

3- Trade-based behaviour (also related to trade-based money laundering)

- Cash payments of high-value orders are an indication of trade-based money laundering (TBML) activity
- Misclassification of gold purity, weight, origin and value on customers declaration forms
- Gold is shipped to or form a jurisdiction designated as 'high risk' for money laundering activities or sensitive/ non co-operative jurisdictions.
- Gold is transhipped through one or more such high risk / sensitive jurisdictions for no apparent economic reason.
- Consignment size or type of commodity being shipped appears inconsistent with the scale or capacity of the exporter or importer's having regard to their regular business activities or the shipment does not make economic sense i.e. there is no reasonable explanation for the client's financial investment into the shipment.
- The transaction involves the use of front or shell companies. Both shell and front companies can be used to facilitate TBML but in different ways. A shell company has no real operating activity and is used to hide money laundering activity and the identities of individuals involved as to obscure the money trial. If activity is traced to the company, it is literally an empty shell.

4- Product differentiation

- The bullion has physical characteristics that are inconsistent with industry standards.
- Gold prices higher than those of the local gold market

5- Payment Behaviour

- A number of affiliated entities in the payment chain.
- Transit movement of funds and changes in purposes of payments.
- Payments to shell companies with further withdrawals.
- Granting of loans (with zero interest rates) to foreign companies.
- Granting of loans (with zero interest rates) to natural persons.
- Natural person or business sells gold saying that it comes from a place with no extractin license or form places with no gold mines.
- Large amount of funds transferred internationally and then withdrawn very quickly.
- International transfers to countries where the company is not registered.
- Significant cash withdrawals from bank accounts by participants within the gold trading industry.
- Division of funds in cheques and smaller cash transactions to pay for merchandise.
- Purchase of gold bullion with bank cheques may be an attempt to conceal the source of the funds and underlying ownership.
- The use of cash to purchase bullion, especially when there are multiple purchases in a short timeframe, or when large amounts are purchased at once, or when there are structured cash deposits into an account to finance a single gold bullion purchase.
- Original source of funds to buy gold bullion cannot be established. The transaction involves the receipt of cash (or by other payment methods, including cheques or credit cards) from third party entities that have no apparent connection with the transaction or front or shell companies or wire instructions / payment from parties which were not identified in the original letter of credit or other documentation. The transactions that involve payments for goods through cheques, bank drafts, or money orders not drawn on the account of the entity that purchased the items also need further verification.
- Transactions between domestic buyers and sellers with sales proceeds sent to unknown third parties overseas.

6- The original crime activity (gold mining)

- Production and commercialisation of gold by a person or business without a license
- An ethnic community hires a third party for the entire operation of the mine
- Licensed mines where the production has decreased with no apparent explanation
- The development of mining activities using machinery and equipment that is not in accordance with the characteristics of the licensed small or artisanal mining
- The development of mining activities without compliance with the administrative, technical, social and environmental regulation.
- The development of mining activities in prohibited areas.

This list of indicators is not an exclusive list. Reporting Entities can identify suspicious transactions involving high-risk individuals, legal entities, and transactions based on other criteria or known indicators of money laundering, terrorist financing, or a predicate offence.