Circular No.(1) of 2020

Reporting Entities Responsibilities in Light of COVID-19 Pandemic

In view of the current national and global crisis due to COVID-19 pandemic and the overall resulting impacts and consequences, including combating financial crimes, the QFIU reminds all reporting entities of their responsibilities pursuant to AML/CFT Law No. (20) of 2019.

Based on the comparative examination it conducted, the QFIU stresses that the activities aiming at exploiting the financial system remain and constantly seek to detect vulnerable areas facilitating access to government systems for abusive and criminal purposes.

Open source information indicates that since the COVID-19 outbreak, some businesses used by illicit actors for money laundering, moved to cash-intensive lines of business to justify the use of the government systems. Other information also highlights that some illicit actors are putting greater focus on the purchase of gold to introduce money in the official monetary system.

In this regard, given the government instructions to reduce the number of manpower working at business premises and remote working situations in the private and public sectors for social distancing purposes, the QFIU emphasizes that reporting entities should continue to implement AML/CFT rules and regulations and identify the transactions that should be reported in accordance with the applicable instructions, where possible. If reporting entities are facing challenges in carrying out their reporting obligations in a timely manner, the QFIU should be notified accordingly in order to obtain the information that would assist the QFIU in performing its functions by virtue of the said Law.

All reporting entities are called upon to inform the QFIU about any unjustified update observed by the entities in terms of the behavior of specific categories of customers when conducting their transactions, or of countries and parties associated with these transactions.

The QFIU refers in Annex (A) to the major proceeds generating crimes which emerged since the spread of COVID-19 pandemic and the implementation of the lockdown criteria by some countries, taking into consideration the daily business procedures of the reporting entities.

Annex (B) outlines some indicators of suspicious activities relevant to COVID-19 pandemic, to be taken into consideration by the reporting entities.

Qatar Financial Information Unit

Annex (A): Major ML/TF Crimes and Risks stemming from COVID-19[1] Pandemic

First: ML Crimes

1. **Fraud and Relevant Activities**

a. Impersonation of government officials:

In such cases, illicit actors contact customers and request their personal banking information, claiming that they work for a government entity. Then they use such banking information to obtain funds in an illegal manner from the victim.

b. Counterfeit goods and products:
This involve goods in general, including essential goods. Whereas in some scenarios goods are delivered but do not meet the agreed standards, or victims are asked to pay the full amount but the goods are never delivered, or are only asked to make an advance payment until the goods are delivered.

c. Fundraising for unlicensed NPOs:
In such cases, illicit actors claims that they work in a non-profit organization. They circulate emails to their victims requesting donations for conducting researches, assisting victims or providing products.

d. Fictitious and fraudulent investment scams:
The promoters of such investments claim that listed companies will invest in products or services aiming at overcoming COVID-19, in order to entice investors to purchase shares in such companies.

e. Drug trafficking, which may involve drug activities conducted online, including using social media, encrypted applications, and "Darknet" markets.

f. Structuring and smurfing schemes, which can prey on economically insecure people who allow their bank accounts to be used in return for a small fee.

2. **Cyber crimes**
    a. Email and SMS phishing attacks

In such cases, cybercriminals send mobile messages or emails to lure victims into clicking links or opening attachments, which enable them to have access to calls directory and data relevant to the victims' personal transactions. The cybercriminals then use such information by impersonating the victims to obtain information from the persons they know to redirect payment transfers.

[1] For more information, please refer to FATF paper on COVID-19- related Money Laundering and Terrorist Financing , Risks and Policy Responses, May 2020.

b. Ransomware attacks:

In such cases, cybercriminals insert malicious viruses on the victims' computers and personal devices to lock access, until the victims pay ransom to the cybercriminals to gain access again to their devices.

Second: Terrorism Financing Crimes

The threats of terrorism financing remain, and terrorist groups may see opportunities for increased terrorist and terrorist financing activity while government attention is focused on COVID-19. The international organizations emphasized in particular the risks relevant to Sahel region (African Coast).

Annex (B) Most Common Indicators of COVID-19 Pandemic

These indicators represent the most common indicators detected. It is worth noting that an indicator does not necessarily mean that the relevant transaction is suspicious, but would rather call for the implementation of further due diligence to know whether any suspicious elements are available and require reporting to the QFIU:

1. Purchase of real estates or troubled businesses to introduce illicit proceeds into the formal financial system.
2. Attempt to restructure indebtedness, in particular bad debts.
3. Attempt to bypass CDD measures by exploiting temporary challenges in internal controls of financial institutions caused by social distancing situations.
4. Increased misuse of online financial services and virtual assets[2] to move and conceal illicit funds.
5. Exploiting economic stimulus measures and insolvency schemes as a means for legal persons to conceal illicit proceeds.
6. Misuse and misappropriation of international humanitarian aids and emergency funding, by avoiding standard procurement procedures.
7. Criminals and terrorist financers move into new cash -intensive and high liquidity lines of business in developing countries.
8. Criminals and terrorist financers fraudulently claiming to work with non-profit organizations to raise funds online.

[2] Please refer to the relevant circular issued by Qatar Central Bank.