

**A study on:**

**Coronavirus Pandemic (COVID-19) and its impact on AML/CFT systems in the Middle East and North Africa Region- Update**

**November 2021**



MENAFATF is considered of a voluntary and cooperative nature, independent from any other international body or organization. It was established under an agreement concluded between its member countries' governments, not based on an international treaty. It determines its own functions, rules and regulations as well as its own procedures, it also cooperates with other international bodies, especially FATF, in order to achieve its objectives.

For more information on MENAFATF, please visit the following website: <http://www.menafatf.org/>

© 2021. MENAFATF

All right reserved No reproduction or translation of all, or part of this publication may be made without prior written permission from MENAFATF, P. O. Box: 10881, Manama, Kingdom of Bahrain, Fax:0097317530627; E-mail address: [info@menfatf.org](mailto:info@menfatf.org)



A study on:

**Coronavirus Pandemic (COVID-19) and its impact on AML/CFT systems  
in the Middle East and North Africa Region- Update**

**November 2021**

Table of Contents

Introduction .....5

Section One: Overview on COVID-19, and its impact on AML/CFT systems through the previous study: .....7

1. Background :.....7

2. Summary of the previous study issued by MENAFATF in the area of ML/TF risks associated with Coronavirus (COVID-19), October 2020. ....7

Section Two: Update on Coronavirus Pandemic (COVID-19) and its impact on the AML/CFT systems in the MENA region:.....11

Section Three: Examples of Case Studies regarding ML/TF crimes associated with the Coronavirus Pandemic:.....20

Summary .....26

Recommendations .....27

Annex.....28

## Introduction

In late October 2020, the MENAFATF issued a study on the “Coronavirus Pandemic (Covid-19) and its impact on AML/CFT systems in the Middle East and North Africa region,” which aimed to spot the light on the pandemic risks associated with ML/TF crimes, with an explanation of the resulting effects and how to address them, as well as submitting a presentation clarifying examples of case studies that faced the countries of the region during the pandemic period to benefit from them in developing best practices and supporting their efforts in AML/CFT in the region. The current report contains a summary of the study in its first section.

The current updated version of the previous study comes within the framework of providing support to MENAFATF member countries on developments related to the Coronavirus pandemic (Covid-19) in the area of ML/TF in the Middle East and North Africa region, by highlighting the risks of this pandemic associated to ML/TF crimes, as well as identifying the most important indicators of suspicion that can help in and detecting ML/TF crimes, in addition to a presentation of a number of case studies that faced the countries of the region during the study period. It is worth noting that this report covers the developments that occurred during the period from October 2020 to date.

For the purposes of preparing this report, a dedicated questionnaire was designed to request information and case studies and was distributed to the countries of the MENA region, to identify the emerging effects of the Coronavirus pandemic (Covid-19) on the AML/CFT systems and the most important methods and ways used in committing the relevant crimes. Accordingly, five responses were received from the following member countries: the Republic of Tunisia, the Republic of Iraq, the State of Kuwait, the Lebanese Republic, and the Arab Republic of Egypt. The number of case studies included in these responses amounted to 6 case studies that varied in various fields, as will be detailed through the report.

In its first section, this report includes an overview of the Coronavirus pandemic (Covid-19), and its impact on the AML/CFT systems based on the previous study, including a brief introductory background on the pandemic and the latest global statistics documented by the World Health Organization (“WHO”). The second part of this section is a summary of the previous study that the MENAFATF issued in October last year.

The second section deals with an update of the study on the Coronavirus pandemic (Covid-19) and its impact on the AML/CFT systems in the MENA region, which looks at the recent developments in ML/TF crimes in the MENA, for example, Issues of international cooperation and response to information requests in a timely manner, emerging methods and typologies for ML/TF risks associated with the pandemic, and enhancing the supervision of activities that may be a source of such risks more than others in times of the crisis, such as NPOs and other businesses.

As for the third section, it includes models of case studies, which were selected based on the prevailing patterns of ML/TF crimes at the international level. Similar cases can be used by reviewing the periodic typologies report in its fourth edition of 2020.

In conclusion, this report presents recommendations for this study, related to the application of the requirements of AML/CFT during the pandemic period, according to the outcomes of the analysis as mentioned in the report.

## **Section One: Overview on COVID-19, and its impact on AML/CFT systems through the previous study:**

### **1. Background<sup>1</sup>:**

According to the global health community and sources, the newly discovered and developed Coronavirus is the cause of COVID-19 disease, which is a wide strain of viruses that may cause disease in animals and humans, ranging in severity from the common cold to more severe diseases such as Middle East Respiratory Syndrome (“MERS”). and severe acute respiratory syndrome (“SARS”).

During a year ago, after the publication of the previous study, the cases of COVID-19 infections until 05 November 2021 amounted to about 249,629,025 cases, while the number of deaths reached about 5,049,374 cases, and the number of cases of recovery from the disease reached about 226,022,072 cases (global figures, including The MENA region. For more information on the latest developments regarding the numbers and statistics of the pandemic, you can see the attached link<sup>1</sup>).

### **2. Summary of the previous study issued by MENAFATF in ML/TF risks associated with Coronavirus (COVID-19), October 2020.**

The MENAFATF conducted an ad-hoc study on the Corona virus pandemic and its impact on the AML/CFT systems in the Middle East and North Africa Region during the period of the pandemic and the report was published on the MENAFATF website in October 2020 (<http://www.menafatf.org/information-center/menafatf-publications/coronavirus-pandemic-covid-19-and-its-impact-amlcft-systems>).

The report provides an introductory background of the Corona virus which caused the COVID-19 disease, the latest global statistics on the number of cases and the death toll, in addition to the identification of the main economic and financial sectors which suffered the most and the ML/TF risks during the pandemic, and the main efforts and initiatives made by international and regional bodies in the AML/CFT field, such as the FATF and the FSRBs. The report ends with a presentation of the main challenges facing the AML/CFT systems in the region due to the Corona virus pandemic, together with some recommendations that the member countries can benefit from.

This report is chiefly aimed to provide support to the MENAFATF member countries on the issues related to the Corona virus (COVID-19) pandemic, by presenting the best practices and highlighting its risks and its connection with the ML/TF crimes.

---

<sup>1</sup> <https://www.worldometers.info/coronavirus/>

It also elaborates on the effects resulted by the pandemic and how to counter them, presents several case studies experienced by the countries in the region during the period of the study, identifies the main red flag indicators that can help identify and detect ML/TF crimes and examines the main challenges that hinder these efforts.

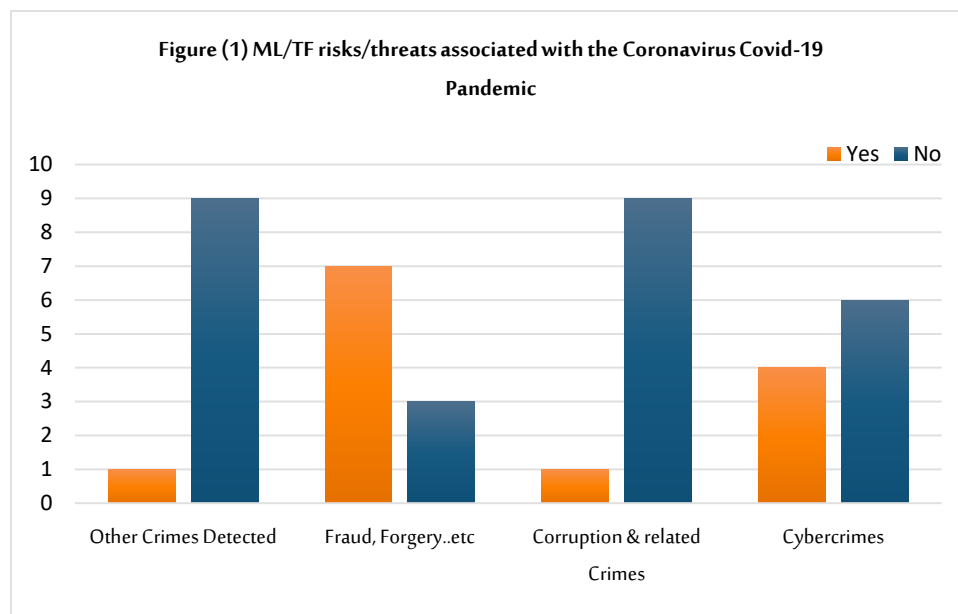
For preparing this report, a questionnaire for the request of information and case studies was designed and distributed to the MENA countries, to identify the effects of the Coronavirus (Covid-19) pandemic on the AML/CFT systems in the region and the most important methods and trends used in committing the related crimes. Accordingly, ten responses were received from the following member countries: The Hashemite Kingdom of Jordan, the Kingdom of Bahrain, the People's Democratic Republic of Algeria, the Republic of Tunisia, the Kingdom of Saudi Arabia, the Republic of Iraq, the Sultanate of Oman, the State of Qatar, the Kingdom of Morocco, and the Republic of Yemen. These responses included 8 case studies that covered various areas, as detailed in the body of this report.

The key findings of the study addressed several COVID19-related money laundering and terrorist financing crimes which were brought into focus by inquiring and examining several global indicators, research and studies issued in this regard and which defined the traits and characteristics of the COVID 19 - related ML/TF risks. It also tackled the rise in the COVID19 - related crimes, such as fraud, cybercrimes, misappropriation, or mis implementation of government funds and international financial aid and corruption.

At the level of the Middle East and North Africa region, according to the facts revealed in the study and the examples of ML/TF risks in times of the Corona virus (COVID-19) pandemic, which were previously mentioned, several crimes such as information technology crimes were detected. 30% of the member countries which responded to the questionnaires reported various forms of cybercrimes which were detected during the period of the pandemic, where methods related to virtual assets and social media were used, such as spreading rumors on medicines that treat the corona virus and practices related to electronic fraud.



The following graph illustrates the COVID 19 - related ML/TF risks in the Middle East and North Africa Region during the pandemic:



The study reached several important points and revealed through the analysis of the cases if none of these points was related to terrorist financing, which means that the MENA region is marked by a low level of TF risks related to COVID 19. It also appeared that the emerging ML risks are not far from what is prevalent worldwide and can be contained and that precautions against their emergence in the future can be taken. It was also found that there are legislative challenges related to the use of technology in committing financial crimes, there are no effective monitoring mechanisms required to implement the existing legislations, particularly in the field of money laundering and terrorist financing crimes and associated offenses, such as fraud and forgery which rank first on the list of cybercrimes and where the use of social media is largely involved; revealing a digital gap and insufficient attention to technology and to its implementation in an effective manner, which clearly varies among FIs more than DNFBPs, thereby affecting the utilization of the e- service platforms.

The study presented many valuable recommendations advising that the objective of the AML/CFT efforts during the pandemic should not only consist of restoring compliance to its former level before COVID-19 but also laying the foundations to strengthen the AML/CFT systems in an on-going and sustainable manner that would respond to times and crisis of the sort. Besides, the times of the pandemic present an opportunity to improve, change and draw the attention to other dimensions, more specifically to digital financial technology, namely at a time where the digital financial services can help contain the spread of the virus, by expanding financial inclusion through the strengthening of financial technology, protecting the financial system, and addressing the vulnerabilities in the financial and economic systems, while keeping risks under control.

The other recommendations that the study comprised included the activation of the international cooperation channels and accurate response to the requests for information in a timely manner by using the available tools to provide international cooperation, while giving priority to urgent requests, the dissemination and exchange of the emerging methods and techniques of COVID 19-related ML/TF risks and sharing them among the international and regional bodies, tightening of control over the activities which may be a source of risk more than others in times of crisis, such as the NPOs. However, their work should not be hampered, and the implementation of the risk-based approach should be observed, especially while implementing the CDD measures, in addition to other recommendations.

The study provided several clarifying examples to deal with some issues related to the implementation of the AML/CFT requirements during the pandemic.

## **Section Two: Update on Coronavirus Pandemic (COVID-19) and its impact on the AML/CFT systems in the MENA region**

MENAFATF plays an important role at the international and regional levels in protecting its member countries and the region as a whole from the ML/TF risks as well as the risks of proliferation financing. Accordingly, the MENAFATF assessed the risks of ML/TF during times of the pandemic to determine the extent to which the AML/CFT systems are affected in the region, and to develop appropriate solutions to meet them and address their effects, especially by addressing some important sectors such as FIs, DNFBPs and NPOs. The MENAFATF issued a report study on the effects of the pandemic as mentioned in the previous section, in October 2020.

In continuation to the role of the MENAFATF as previously mentioned, it has started updating the study represented in the current version a year after the date of publication of the first study, in order to explore and monitor any changes or developments that could affect the patterns, methods and trends of committing ML/TF crimes in the region. The pandemic persists despite fading out, but the danger exists and sometimes expands suddenly, and as a result, the work to combat the Coronavirus pandemic has been extended to varying degrees, in which the degree of precautions varies from one country to another, and from one sector to another within the country, or at the regional and international levels. Trade and economic transactions, travel measures and other aspects were also affected by these measures. However, on the other hand, the ways, and methods of committing ML/TF crimes have changed, in a parallel pace to the variables, if not faster.

To prepare the current study, a questionnaire was designed to request information and case studies, analyze the responses received from member countries and reflect the results reached through several themes that were included in the questions addressed in the questionnaire, as listed below:

### **1. Changes in the ML/TF patterns on the supervisory authorities' AML/CFT systems:**

A sample of the MENAFATF member countries that responded to the request for information and case studies questionnaire in this regard was surveyed regarding their monitoring of any observations or changes in the patterns of ML/TF with regard to the supervisory authorities' AML/CFT systems. The surveyed countries reported with the following:

1. The spread of fraud in various forms through several aspects, such as obtaining financial aids from foreign countries to combat the pandemic - through fraud by submission of false documents, or
2. Establishment of shell companies and seizure of public funds, exploiting the pandemic to conclude deals for supplies of pandemic-fighting equipment, and then evading the deal without completing it, or
3. Companies exposure to electronic fraudulent remittances by electronic means of correspondence by changing the account number of the beneficiary in money transfer form or changing it for the benefit of third parties when opening new accounts outside the country.

4. Regarding changes related to STRs or the STRs reporting process, 60% thereof were answered in (No Changes), while 20% thereof stated that there was a clear increase in the number of STRs received compared to the two years preceding the pandemic. Also, 20% thereof reported that all the STRs were received from banks.

According to the foregoing, we conclude that there is a prevalence of fraud methods during the pandemic period, in which electronic means are widely used due to the tendency of most businesses to conduct their commercial and economic activities remotely, and this includes banks, of course, which had the lion's share of targeting money launderers and financiers of terrorism, where most of the operations were associated with Bank fraud in one way or another. On the other hand, it can be considered that the changes in STRs and its reporting processes are somewhat normal due to the absence of a clear increase or decrease, but it is more likely that there are no changes, given the proportion of countries that responded in negative change thereof, which amounted to 60% as mentioned above.

## 2. Changes in ML/TF Patterns in the Reporting Sectors:

The previous study conducted by the MENAFATF, published in October 2020, acknowledged the existence of various forms of cybercrime that were monitored during the pandemic period, for example, virtual currencies crimes, and the spread of rumors on drugs that treat the Coronavirus and other fake news through social media, as well as practices related to fraud and electronic fraud particularly through the use of social networking sites to steal the data from electronic wallets of customers and withdraw money therefrom later.

When surveying the MENAFATF countries about the presence of changes in these patterns during the current study period from August 2020 to date, 60% of the surveyed sample stated that no relevant changes were observed. While 40% of the sample reported an increase in crimes related to extortion through electronic payment methods, an increase in transfers under simplified CDD measures, and an increase in fraud through electronic transfers generally. In addition, the same patterns were observed indicating regular and cyber fraud, patterns related to the misuse of pandemic assistance such as the establishment of shell companies for the purpose of carrying out fictitious operations to obtain pandemic aid funds, and fraud in counterfeit merchandise/goods in medical products used in combating the Coronavirus pandemic.

As for the NPOs sector, despite the vital and important role it plays in times such as the Coronavirus pandemic, and that it may be one of the most vulnerable to risks and exploitation, there was no indication of the exploitation of this sector, contrary to the results of the aforementioned study, which acknowledged the existence of practices associated with individual cases, personally aimed at collecting funds for potentially legitimate purposes, but the necessary permit/license to collect donations was not obtained from the concerned authorities.

3. **Threats and risks expected to occur later according to the current prevailing patterns and trends of ML/TF crimes related to the Coronavirus pandemic:**

In times like the Coronavirus pandemic, there are many possible threats which were mentioned through reviewing of a sample of specialized studies and reports, where some crimes related to ML/TF, which are likely to be linked to risks/threats related to the Coronavirus pandemic to a large extent, were addressed, for example, it had been noticed that there is an increase in the number of electronic fraud, counterfeit of goods/merchandise in medical products used in response to the Coronavirus pandemic, and other threats.

60% of the countries surveyed revealed that they do not face challenges in mitigating potential risks and threats related to ML/TF related to the Coronavirus pandemic (COVID-19). And 20% thereof reported similar threats, including the high rate of cybercrime, and the increase in fraud cases in counterfeit of goods, especially medical products used to face the crisis. Also, 20% of countries reported that related threats are to money-related crimes in general but not specifically.

40% of the surveyed countries unanimously agreed that there are challenges facing the institutions concerned with addressing these threats represented in the insufficiency of electronic capabilities and technologies in FIs and their branches, which are used to detect the occurrence of ML/TF crimes related to the Coronavirus pandemic, and insufficient human resources qualified to deal with modern electronic technologies exploited in the implementation of ML/TF operations, in addition to the lack of well-studied plans to help detect ML/TF operations in light of the pandemic.

4. **Regulatory and procedural regulations issued by the authorities responsible for implementing and applying ML/TF requirements and standards regarding ML/TF risks related to the Coronavirus pandemic:**

The countries that were surveyed interacted with the Coronavirus pandemic positively, by issuing bulletins, regulations and other relevant publications, as one of the countries rushed to issue a circular addressing banking and non-banking FIs to take highly precaution measures on the financial transactions that are made by them on bank accounts and electronic wallets, and electronic payment cards, as well as exploiting social media pages, especially those associated with celebrities, and urging the development of scenarios for detecting ML/TF in proportion to financial transactions. These authorities have also been encouraged to take the required EDD measures particularly against the online shopping (e-shopping and online marketing website) owners financial transactions. Whereby a circular and a guidance paper was issued by the FIU on the ML/TF risks related to the Coronavirus pandemic.

Second country carried out the following procedures:

- Raising awareness in the private sector based on the paper issued by the FATF on the COVID-19 related Money Laundering and Terrorist Financing Risks and Policy Responses and published it on the FIU's website.
- Raising awareness among the FIU's employees and providing them with the paper issued by the Egmont Group on Covid-19 best practices for financial intelligence units.
- The Customs' implementation of a plan to combat smuggling and counterfeiting that includes sterilization products and protection against the Coronavirus, to reduce forgery crimes (counterfeiting sterilization and protection products and falsifying the results of PCR tests and vaccines), as the concerned authorities conducted periodic inspections in all regions to detect counterfeit products and track their sources.
- The LEAs concerned carrying out raids to seize and confiscate counterfeit products.
- A mechanism has been put in place with strict controls, to prevent the misuse of grants and donations related to fighting Coronavirus.

A third country issued a circular regarding dealing in the real estate sector during the pandemic, stipulating the commitment of the real estate registration and documentation departments before obtaining the signatures of the stakeholders on the documents and contracts, to ensure that a copy of the bank transfer is attached stating the purpose of the transfer of funds or a copy of the certified cheque through which the payment was made. On the other hand, the Ministry of Interior was directed to issue a decision prohibiting the transfer of vehicles title without attaching bank receipts that prove the legitimacy of the funds, which mitigates ML operations.

With regard to conducting offsite and onsite supervision operations, compliance with the requirements of social distancing required in light of the Coronavirus pandemic was taken into account by reducing the number of onsite inspectors, in the tasks that take place within local banks, as well as carrying out inspection tasks for exchange companies (remotely) at the headquarters of the Central Bank, by requesting for information and documents from the units subject to the supervision of the Central Bank to be examined in the office, and communication with these units is carried out remotely in the event of requesting any additional information, provided that the presence at the headquarters of the unit subject to inspection is within a maximum period of 3 working days until health conditions improve. The Central Bank has also issued instructions related to the use of customer identity verification through the application available on smart mobile phones, and the subject units have also been instructed on the requirements to be considered in services and dealing with customers, especially how to complete KYC data via modern financial technologies (EKYC) and its requirements for verification of customers.

A fourth country reported that, in the context of raising awareness of best practices to address the Coronavirus pandemic, it issued a circular to the reporting entities, which includes many measures to be taken in this regard, most notably the following:

- Applying EDD measures regarding financial transfers related to the Coronavirus pandemic, when the customer changes the beneficiary account number of incoming and outgoing money transfers to the country.
- When there is a suspicion that the customer's email has been hacked, with what is known as "Business Email Compromise," the required transfer must be refrained from being made and an STR of fraud must be submitted when necessary.
- Pay special attention when analyzing the financial flows of persons and companies who have received transfers from foreign countries, suspected of being related to funding and assisting from foreign countries, international organizations and other donors related to the Coronavirus pandemic, and immediately report an STR when necessary.
- Applying EDD measures regarding the financial transfers associated with the Coronavirus pandemic, when PEPs interfere in the purchase of medicines or other medical or non-medical supplies, and immediately report an STR when necessary.
- Carrying out continuous monitoring of the financial businesses of companies active in the sectors most affected by the Coronavirus pandemic.
- the risks associated with the Coronavirus pandemic must be included in customers' risks matrix, the activities they carry out and the banking products they request, or when providing any facilities regarding the request for basic documents to verify the identity of the customer or the company within the framework of the CDD measures, and update the risks of the related customers without delay, and report STRs when required.
- Adding the following phrase "COVID19" when reporting the relevant STR.

Finally, a fifth country reported that the Central Bank had issued instructions and procedures to limit the effects of the emerging coronavirus and extended the work of some exceptional measures for additional periods to urge customers to use electronic services and achieve financial inclusion. Among those services, we mention:

- Exemption from commission against bank transfers.
- Issuing free electronic wallets.
- Exemption from transfer fees between electronic wallets.
- Issuing free touchless prepaid cards.

Also, among the measures taken by this country, the FIU issued a guidance paper to FIs, DNFBPs and the supervisory authorities on "ML/TF risks associated with the spread of the emerging coronavirus" and published it on the FIU's website. Regarding non-bank financial institutions, the supervisory authority has developed a package of initiatives to facilitate customers' transactions, and work on the safety and stability of non-bank financial markets, including the capital market, insurance services, real estate financing, financial leasing, and factoring.

5. **National coordination and cooperation between local authorities responsible for implementing and applying ML/TF requirements and standards:**

Coordination at the level of all national bodies concerned with AML/CFT continued naturally during the period of the Coronavirus pandemic through various forms of cooperation and coordination, for example, training webinars were held on many topics in the field of AML/CFT, due to non-conducting interactive (face-to-face) training activities which were stated training plan dedicated to its human cadres working in banking and non-banking financial institutions, and familiarize them with the most important ways and methods used in the implementation and commission of these crimes during the pandemic.

Also, there is continuous cooperation with the local authorities in AML/CFT matters through the electronic linkage between the FIU and some of the main entities with relation to AML/CFT.

Furthermore, Communication between the public and private sectors was also conducted during the pandemic period between the relevant authorities of government agencies and the reporting bodies from the financial sector, and DNFBPs to work on updating policies and procedures to mitigate the risks.

In addition to the above, and in line with the possible repercussions of the spread of the Coronavirus, coordination has been made to take some exceptional measures related to stimulating the use of electronic means and channels for payment, in addition to exceptionally allowing the implementation of customer identification procedures when opening new accounts via mobile phone or via other similar electronic means.

In general, a number of the surveyed countries reported the existence of coordination through the national anti-money laundering and terrorist financing committees, as well as direct communication that takes place, whether through bilateral correspondence or memorandum of understanding between the different parties represented in the committees' membership in the field of cooperation required regarding AML/CFT efforts, thus, there is cooperation and good coordination between the various authorities in the field of implementation and application of ML/TF requirements and standards.

6. **Relationship with the private sector and the bodies responsible for implementing and applying ML/TF requirements and standards:**

In its response to the relationship between the public and private sector and the authorities responsible for implementing AML/CFT standards issued by the competent authorities, such as FIUs, central banks and others, 80% of the sample surveyed reported the existence of close cooperation between the public and private sectors. In this regard, the importance of the obligation of the reporting bodies to implement AML/CFT systems, in particular the reporting of STRs, was emphasized, and

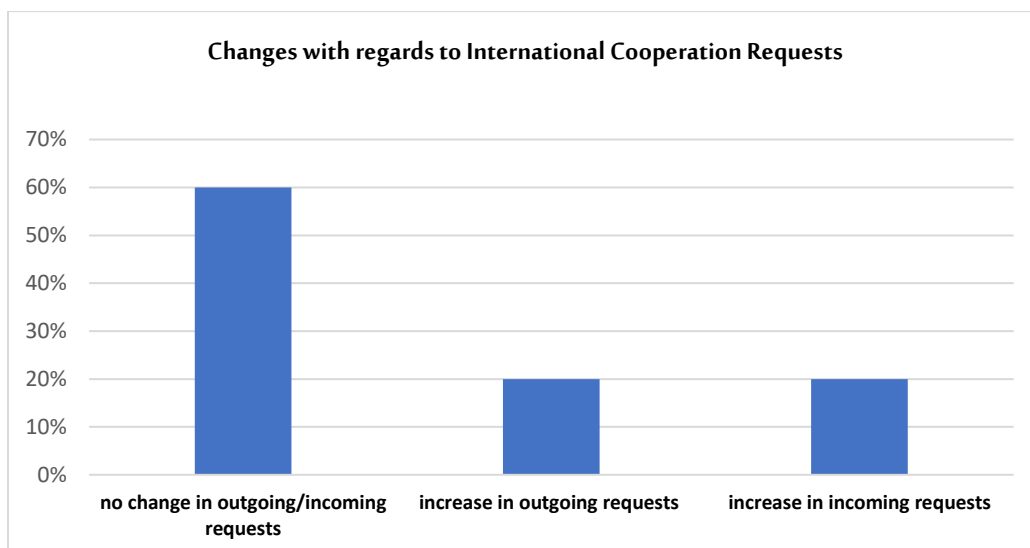


directives were issued in the same context to report to the FIUs in the event of any obstacles or challenges facing these institutions in reporting.

In the field of offsite and onsite supervision, 40% of the sample surveyed reported that the work of the offsite and onsite supervision is being carried out regularly, considering the imposed health precautions, as onsite inspections are carried out in accordance with the safety and prevention measures in place, and in coordination with the relevant reporting authority. On the other hand, the obligated institutions provide the concerned authorities with all the information and data they request within the specified deadlines, and these entities are also provided with instructions to combat money laundering and terrorist financing in accordance with the prevailing conditions and consistency with the requirements contained in the standards issued by the FATF Financial Action Group. In the same context, training courses and workshops are held in the field of combating money laundering and terrorist financing to spot the light on any matters or developments related to the pandemic, or through the results of the follow-up that is carried out through field and office monitoring carried out by the supervisory authorities.

7. **Change in requests for international cooperation related to ML/TF cases related to the Coronavirus pandemic during the specified period:**

60% of the responses reported that there was no noticeable change in requests for international cooperation related to ML/TF matters during the pandemic period. While 20% reported an increase in information requests received by counterpart FIUs, revolving around fraud through remittances, especially those executed through international money transfer companies, and the exploitation of social media in fraud operations was also noted. Moreover, 20% thereof reported an increase in outgoing requests. The figure below shows the changes related to international cooperation requests related to ML/TF cases related to the Coronavirus pandemic during the specified period:



As for the timely response for information requests, the responses received indicated that the impact of the Coronavirus pandemic causing a delay in response due to the impact of the counterpart FIUs by partial closure/lockdown, complete closure, or completion of the work of the FIUs remotely and the inability to obtain the required information from the competent authorities on time due to this impact. The other reason is due to the precautionary measures taken by some countries to confront the pandemic.

#### 8. **Measures to be taken to mitigate the effects of the Coronavirus pandemic:**

Through the study, several important measures recommended by the sample under study were monitored to mitigate the effects of the Coronavirus pandemic to reduce the related ML/TF risks, which included the following:

##### Financial Institutions:

1. Work on setting controls, providing and developing sufficient capabilities and equipment to provide financial services remotely through modern financial technologies, including mobile phone applications and Internet banking, while providing various means to educate customers on how to use these methods safely.
2. The need to follow the RBA approach (classifying customers according to their level of risk) in order to determine the CDD measures based on those risks, and encouraging FIs to carry out EDD measures towards the financial transactions executed especially electronically.
3. Directing FIs on the requirements to be considered in services and customers transactions with regards to completing Know Your Customer data through modern technologies (EKYC) and the procedures required for identity verification.
4. Increased interest in providing appropriate remote training programs on AML/CFT for employees of the FIs, including the potential threats and risks because of the spread of the virus, and indicators of suspicious operations related to exploiting its spread.
5. Increased interest in following up the extent to which the sectors and branches of the FIs comply with the requirements of AML/CFT.
6. It may be appropriate to issue guidance to increase attention to certain situations that require special attention, for example the following:
  - Applying EDD measures regarding financial transfers related to the Coronavirus pandemic and monitoring any signs of suspicion observed about the customer changing the account number of the beneficiary from and to the country, for example.
  - Upon suspicion of customer's e-mail has been hacked with what is known as "Business Email Compromise," completing the required transfer must be refrained from and an STR must be reported.
  - Pay special attention when analyzing the financial flows of persons and companies who have received remittances from foreign countries, suspected of being related to funding and assistance from foreign countries, international

organizations and other donors related to the Coronavirus pandemic, and immediately reporting an STR when necessary.

- Applying EDD measures regarding financial transfers related to the Coronavirus pandemic, when PEPs interfere in the purchase of medicines or other medical or non-medical supplies, and immediately reporting STR when necessary.
- Conducting continuous monitoring of the financial activity of companies active in the sectors most affected by the Coronavirus pandemic.
- Including the risks associated with the Coronavirus pandemic in the matrix of customers' risks, the activities they carry out and the banking products they request, or when providing any facilities regarding the request for basic documents to verify the identity of the customer or the company within the framework of the CDD measures and updating the risks of the related customers without delay and reporting STR when appropriate.

Law Enforcement Authorities:

- It is recommended to focus more in the current period on combating the crimes associated with the spread of the virus and applying its precautionary measures, and allocating sufficient and appropriate resources in this regard, with the need not to affect the fight against other serious crimes (such as collecting donations for fake charitable institutions or without a license, impersonation of officials' personality).

Supervisory Authorities:

1. Relying on appropriate means that enable remote monitoring in the field of AML/CFT during the crisis period, such as the use of video conferencing technology.
2. Giving more flexibility to the authorities and sectors in submitting some reports and data that are not related to office supervision, as it is possible to limit the provision of some reports and data, and consider extending the deadlines for providing others, and exemption from submitting certain reports and data, all according to the importance and nature of reports and data and to according to the supervisory authority's discretion and according to the degree of risk and the relative importance associated with the requested reports and data to be submitted.

## **Section Three: Examples of Case Studies regarding ML/TF crimes associated with the Coronavirus Pandemic:**

As explained in the introduction to this report, the case studies included in this report represent a sample of cases related to ML/TF crimes related to the Coronavirus pandemic, an estimated number of which were addressed in the body of the periodic typologies report (Biennial report) fourth version of 2020, which was issued concurrently, on the same date, with this report. The said report can be viewed for more information, if so necessary.

### **Case Study No. 1: Manipulating papers and submitting false documents**

The suspected person, is of a foreign country's nationality, accompanied by four persons, visited the branch of the reporting bank, and met with the branch manager to open an account that will have an investment transaction volume of about USD 500 million. The transaction will be the establishment of laboratory to conduct Covid-19 rapid tests. The suspect submitted a copy of an authorization letter (not attested) issued to him by a person from another foreign country nationality ("Principal"), authorizing the suspect to manage the principal's accounts internationally, due to the principal's health conditions that prevent him from traveling as a result of being infected with COVID-19. When asked about the source of the funds (USD 500 million) and the supporting documents therewith, the suspected person stated that such documents are not currently available and requested to open the account and provide the bank with the required documents later.

Suspicion Indications on the case were:

- The volume of the amount of which the notified person stated that he intends to invest without any indications of his financial solvency.
- Lack of clarity about the actual purpose of opening the account.
- Suspicion of submitting false documents.

The results of the FIU's analysis, after referring to open information sources, indicated that the suspected person is the CEO of a bank, and it was found that there was bad news of him being an ex-prisoner for collecting donation funds for a fictitious purpose, and using pseudonyms for the purpose of borrowing and benefiting from housing loans privileges.

Considering the previous data, the bank refused to carry out any financial transactions related to the person. Information was requested from two counterpart FIUs; one of the aforementioned person's nationalities, and the other of the principal's nationality. LEAs were contacted to conduct their investigations.

The predicate offenses were fraud and forgery. The case is under examination and investigation.

**Case Study No. 2: Concluding business deals for the supply or manufacture of anti-regulation requirements**

The suspected person, who holds the nationality of a foreign country, has opened an account with the reporting bank. He stated that he works as an advisor to an international bank, and that the purpose of opening the account is to receive monthly salary transfers, and that he has worked in several different institutions in many countries, whereby he will receive an incoming transfer on his account from a law firm in a foreign country, amounting to about USD 4.1 billion, as payments to a sales commission for concluding a commercial transaction, to supply (gloves/clothes/medical masks) used to deal with COVID-19. Upon receipt of the aforementioned transfer, he will transfer half of the amount to the account of his partner X (holds of the same nationality of the suspected person).

Suspicion Indications on the case were:

Lack of clarity about the actual purpose of opening the account.

Lack of documents supporting the source of the said amount.

The volume of the transaction value and the amount of the commission, are not in line with the KYC documents of the suspected person.

Failure to verify the actual purpose of the person's residence in the country.

The results of the FIU's analysis showed that the suspected person holds the nationality of a foreign country and is (a non-resident customer), as his residence is registered to a hotel in the country. He also submitted an agreement form between him and the company that is to transfer the amount of his commission, without the signature of any parties, which raises doubts about its authenticity.

Considering the above information, a letter has been written to the FIU of the suspected person's country, in order to obtain the information available thereto on the suspect, and that there is an expected transfer will be received from the same country. LEAs were also contacted to conduct the necessary investigations.

The predicate offense was fraud, and the case is under examination and investigation.

Case Study No. 3: Supplying medical devices

The FIU received an STR from a bank about a sole proprietorship established in 2013, with a capital of USD 3,172, its activities are import, export and public supplies, where a transfer to its account of about USD 2.1 million was received from a foreign company abroad. This transfer coincided with the FIU's receipt of information request from a counterpart FIU regarding the same entity in question, due to its suspected involvement in a possible fraud related to the supply of medical devices used to deal with the COVID-19.

Indicators of suspicion in the case were represented in the large amount of transfer received to the account of the suspected proprietorship, which is not commensurate with the historical movement on the account, in addition to the receipt of information from a counterpart FIU on suspicion of possible fraud related to the supply of medical devices considering the COVID-19.

The results of the FIU's analysis indicated that the owner of the suspected proprietorship stated that the purpose of the suspected transfer was that he had contracted with a foreign company to export goods abroad (COVID-19 masks), and that he did not fulfill the requirements of the contract due to the issuance of decisions that prevent the export of such medical supplies abroad, thus he will export - by shipping - the goods directly from abroad to the importing company abroad.

Based on reviewing open sources of information, it was found that the transferring company recently was awarded a general contract related to the supply of COVID-19 protective masks in an infected country, and the same country has recently fallen victim to a possible fraud in the supply of masks.

The counterpart FIU was responded to with the available information, and a letter was written to LEAs to conduct their investigations.

The predicate offense was fraud, and the case is under examination and investigation.

Case Study No. 4: Forgery of commercial papers and invoices

The FIU received an STR related to an electronic fraud where a local company “A” fallen a victim for, whereby the grounds for the STR were summarized that the concerned company carried out a commercial transaction during November 2020 represented in importing “COVID-19 Virus Analysis Reagents” from company “B” located in the country “Y”, the purpose of the transaction was indicated in the invoice, which includes the bank statements of this company. However, prior to making the payment, the local company received several electronic communications appeared to be from the e mail of company “B” requesting to change the bank details contained in the relevant invoice, and to transfer the amount of payment of the said invoice, estimated at USD 311 760.00, to a bank account in country “X”.

Following the completion of the transfer, to the account opened in country X instead of the account opened in country M, it was noticed that the supplier did not actually write [the email] to the local company, and therefore did not receive the amount that was the subject of the transaction. It is likely that the email was hacked with the aim exploiting it to send fake e mails, which is known as "Business Email Compromise".

As a result of the correspondence with the counterpart FIU in country X, it was found that the actual beneficiary of the transfer was someone who had established a shell company “B” with a name completely similar to company “A” and then hacked the e mail of this company to send fake electronic correspondence and be able to benefit from a financial transfer without rightly so. As soon as this transfer was received, the person concerned withdrew it the transfer in cash and subsequently closed the account. The counterpart FIU also reported that it had received an STR regarding the bank transfer received by the account of company “B” issued by the local company, estimated at USD 311,760 USD.

The FIU informed the Attorney General of the matter as well as of the merits of the fraud. The reporting bank was also informed of this statement, while directing a warning to the bank due to not considering the EDD measures upon verification of international transfers under the title of “payment against imports in connection with the COVID-19”

Case Study No. 5: Execution of contracting projects

The FIU received an STR that the bank account of Company (A) belonging to the defendant "A.H" with total amounts estimated at about USD 2,481,899 coming from the consulate of a foreign country within the framework of a contract concluded between the two parties for the purpose of providing the stranded citizens of a foreign country in our country with medicines and tests to diagnose COVID-19. The transfer had to be transferred (15% of the amount to be paid as bills for hotels clinics and pharmacies within the framework of the implementation of the contract whilst the rest of the amount to be transferred to the personal account of the defendant so called "A.H" and other different accounts opened in the names of natural persons and a sister company (company "B") in addition to the account of company "C" also belonging to the defendant "A.H" in which [Company C] an STR was filed after receiving five identical and partial transfers from company "A" on the same day for a total amount of USD 141,952.

Through the investigations carried out by the FIU it was found that the contract concluded between the so-called "A.H" and the consulate does not explain the services required from the company or the prices it was also found that the transfers were made from the account of company "A" to the benefit of company "B" based on forged invoices containing abnormally high prices and as a result of these indicators it was found that the so-called "A.H" is intending using a fictitious company "A" in addition to companies owned by his family members in which issued forged invoices to embezzle public funds allocated by a foreign country to its citizens stranded in our country due to a COVID-19.

Accordingly, the FIU authorized the freezing of the accounts of companies "A", "B" and "C" and the personal account of the defendant "A.H" and referring the file to the Public Prosecution for action. The FIU within the framework of international cooperation directed spontaneous disclosure to the Foreign FIU.



**Case Study No. 6: The exploitation of financial aid provided in the context of the pandemic**

The FIU received a request for information from a foreign FIU regarding investigations carried out on the so-called A.H (a citizen residing in a foreign country) and his company X (a company registered in a foreign country established on () and active in the field of construction and public works). The request stated that the personal account of the named A.H was fed with USD 980,252, received from a public department in a foreign country. These amounts were originally sent to company X's account within the framework of financial aid to companies during the COVID-19 crisis, but the investigations revealed that the so-called A.H carried out a fraudulent act to collect these funds in his personal account in France, he collected these funds by virtue of several partial transfers with a total value of about USD 149,976, against his personal account opened with a local bank at No. 1.

By investigating the designation of the funds received in the account, it was found that he transferred them to two accounts opened in his name with the same bank:

4 transfers worth USD 132,970, to his account 2, he withdrew amounts of USD 8,532 in cash and made transfers worth USD 117,327, the most important of which went to a person named Khaled worth USD 37,331, a transfer to R.A.(titled: purchase of an apartment) with a value of USD 71,107 and a transfer to his account 3 in the amount of USD 3,555.

4 transfers, amounting to USD 1,063,743, to his account 3, of which he withdrew in cash.

Whereas it was found that the funds collected by the concerned person resulted from a fraud act that he carried out to change the destination of the financial aid provided by the authorities of the foreign country in the context of the COVID-19 crisis to his personal account instead of the account of his company X.

The act went through the three stages of money laundering:

Placing: Collecting undue sums resulting from the fraud and forgery of documents.

Disguise: Making many transfers into many accounts between the country and several foreign countries in order to separate them from their main source, in addition to dividing them in order not to arouse suspicions.

Integration: The purchase of property of amounts generated illegally.

## Summary

1. It became clear through the analysis, that the findings of the current study confirm what was concluded for in outcomes and findings of the previous study of the MENAFATF published in October 2020. The changes that occurred are minor ones and are in line with the current developments in the MENA regarding ML/TF crimes related to the Coronavirus pandemic. These changes do not constitute a noticeable difference from what was previously observed, except in some points, as will be shown below.
2. The report clearly showed, through the cases analysis, that emerging ML risks are linked to fraud as a predicate offense for ML crimes, and this is one of the current trends at the global level, according to similar and specialized studies.
3. It is noted that during times of the pandemic, the criminals mainly tended to the banking sector, which was concluded through the analysis of the case studies received, although the sector is considered one of the strongest fortresses for money launderers, but it remains the first target for the destination of their dirty money.
4. It is noted that the methods tend towards the use of technology mainly, which drew the attention of the authorities concerned with AML/CFT to the need to reconsider international laws and standards to suit similar conditions that may occur in the future. As crime continues to evolve and keep pace with the latest technical developments, rather it is ahead of the competent authorities concerned with AML/CFT, which poses a challenge thereto and calls for the increase in its human, material, and technical capabilities, which requires that the world be prepared for this by providing tools and legislation from now on.
5. There are still legislative challenges when using technology to commit financial crimes, and the lack of effective supervisory mechanisms required to implement the existing legislation, especially in ML/TF crimes, and related crimes such as fraud, which occupy the largest share in the list of crimes committed electronically, where Social Media overlaps in a large percentage.
6. The challenges of working remotely have proven the possibility of continuing good cooperation and coordination between the authorities concerned with AML/CFT, and it has also become clear that this situation has not severely affected the effectiveness of supervision over these businesses, especially in FIs.
7. In the case studies contained in the report, there were an estimated number of suspicious indicators that could help in identifying and detecting suspicious activities related to ML/TF operations related to the pandemic, among which we mention the following:
  - I. Forgery of contracts and manipulation of official papers.
  - II. Outgoing/Incoming money transfers.
  - III. The nature of the actual activity is different from the licensed one, or the actual activity is not clear.
  - IV. Exploiting social media to raise funds.
  - V. Transfers between accounts (i.e. accounts as point of deposit, and the transfer of funds occurs to other accounts).
  - VI. Failure to obtain documents or provide convincing justifications for the financial transaction(s).

## Recommendations

Through what was reviewed in the report, and through analyzing the information contained in the responses received from the participating countries regarding the request for information questionnaire, some recommendations were reached to assist the competent authorities in their efforts to address ML/TF risks considering the Coronavirus pandemic, as follows:

1. Emphasis should be placed on strengthening the AML/CFT systems on a continuous and sustainable basis so that they are not vulnerable to infiltration in times of the crises similar to the pandemic or otherwise, and attention should be paid not to over-supervise the compliance with the AML/CFT standards in all financial and non-financial sectors with a focus on the banking sector.
2. Ensuring that controls are in place to provide and develop sufficient assistance to provide financial services remotely through modern financial technologies, including mobile phone applications and Internet Banking, while providing various means to educate customers on how to use these methods safely, and the need for a form of coordination with Internet Service Providers and modern financial technology service providers to support the use of digital identity and combat electronic fraud.
3. The necessity of following the RBA (classifying clients according to their level of risk) to determine the CDD measures based on those risks, and to encourage FIs to carry out EDD measures towards financial transactions executed electronically, especially the completion of Know Your Customer data through modern technologies (EKYC). and its requirements to verify identity.
4. Enabling financial technology and protecting the financial system, as well as addressing vulnerabilities in the financial and economic systems while keeping risks under control by relying on appropriate means that enable remote monitoring in AML/CFT during the crisis period, such as using video conferences technology.
5. Increasing interest in providing appropriate remote training programs in AML/CFT for employees of FIs, including the potential threats and risks because of the spread of the virus, and indicative indicators of suspected operations related to exploiting the outbreak thereof.
6. Reviewing the adequacy of AML/CFT controls and their conformity to meet critical and crisis conditions, such as the Coronavirus pandemic, and ensure that they meet the aspects related to the use of technology with appropriate mechanisms to apply them to ensure that economic activity packages are not abused.

## Annex

### **A questionnaire for requesting information and case studies regarding the update on Coronavirus Pandemic (COVID-19) and its impact on AML/CFT systems in Middle East and North Africa Region**

- a. This questionnaire comes within the framework of completing the previous study carried out by the MENAFATF on the Coronavirus Pandemic (COVID-19) and its impact on AML/CFT systems in Middle East and North Africa Region covering the period from August 2020 up to date.
- b. Based on the aforementioned study on the [Covid-19 and its impact on the AML/CFT systems in the Middle East and North Africa region](#), please kindly respond to the following questions while providing as much information and case studies as possible.

#### **Questions:**

1. With regard to the supervisory authorities on AML/CFT systems, have any changes in the patterns of ML/TF related to the COVID-19 been monitored during the period from October 2020 to date, please provide a clear and concise description (supported by statistics or case studies, if any) that highlights the most important of these changes, by classifying them to (ML, TF), with regard to the following authorities:

- FIU (number of STRs, reporting entities, most reporting sectors...etc);

LEAs (the most frequent crimes, the sectors in which crimes are committed, the classification of crimes, especially the size and type of financial crimes, in general, all crimes related to the ML/TF predicate offenses, .....etc);

Judiciaries (for example, specialized prosecutions such as the Anti-Corruption Prosecution and ML/TF prosecutions...etc.);

Supervisory authorities (the Central Bank, and the supervisory authorities on securities and insurance sector.... etc).

2. As for the reporting sectors, and in accordance with question (1) above, please provide a clear and concise description (supported by statistics or case studies, if any) highlighting the most important of these changes in a categorized manner (ML, TF), as listed below (changes may include change in the pattern of crimes committed in the implementation of ML/TF operations, such as the increase in electronic crimes, fraud, forgery, fraud in counterfeit and fake goods in medical products used to encounter the COVID-19, and other crises).

**Sectors:**

- I. **Charities and NPOs:**
  - II. **Institutions of financial sector such as banks, exchange houses, money transfer companies, securities, insurance and others:**
  - III. **Sectors related to DNFBS (as set out in the 2013 FATF Compliance Methodology and its subsequent amendments):**
  - IV. **Predicate offenses related to ML/TF crimes:**
    - Information technology crimes (electronic and cybercrime (text messages, calls, piracy, account hijacking, attacks on financial services companies.... etc.);
    - Fraud, counterfeiting and fake in products used in response to the pandemic (collecting fake donations, manipulating markets and prices of some goods... etc.);
    - Corruption, in particular cases related to the public sector (job abuse, misuse of pandemic aids, theft and misdirecting the aids destinations, accepting bribes.... etc.);
    - Others (remember):
3. **In your opinion, what are the threats and risks expected to occur later, according to the current prevailing patterns and trends of ML/TF crimes related to COVID-19?**
  4. **Have any regulatory or procedural regulations been issued - by the authorities responsible for implementing and applying ML/TF requirements and standards as a result of the impacts of the COVID-19 or to deal with ML/TF risks related to the pandemic - to mitigate, prevent, or to help discover them? (Please attach a copy if the answer is yes).**
  5. **Were any penalties imposed by the supervisory authorities against the reporting entities and affiliated ones as a result of violating the rules and procedures of AML/CFT related to dealing with the pandemic? (Please attach a copy of it if the answer is yes).**
  6. **In your opinion, how would you describe the results of national coordination and cooperation between the local authorities responsible for implementing ML/TF requirements and standards, while providing examples of best practices, if any?**

7. In your opinion, how would you describe the relationship with the private sector and the bodies responsible for implementing and applying ML/TF requirements and standards, while providing examples of best practices, if any?
  
8. Were any changes monitored regarding requests for international cooperation related to ML/TF cases with relation to COVID-19 during the specified period?
  
9. Do you have suggestions regarding the measures to be taken to mitigate the effects of the COVID-19 with regards to AML/CFT measures? Or any other general suggestions?

A template for submitting case studies related to ML/TF in light of COVID-19

<b>Brief of the Issue</b>	
<b>The type of entity that was exploited in the case (bank, money exchange, etc.)</b>	
<b>Tools and methods used in the case</b> (Cash, cheques, transfers, virtual currencies...etc).	
<b>Indications of suspicion associated with the case</b>	
<b>The results of the analysis or investigations on the case</b> <b>Please indicate the amount(s) under investigation/confiscation</b>	
<b>Predicate offense and legal status of the case</b>	



November 2021

