



JOINT GUIDANCE ON THE TREATMENT OF FINANCIAL CRIME RISKS AND OBLIGATIONS IN THE UAE IN THE CONTEXT OF THE COVID-19 CRISIS

5 May 2020

The content of this Joint Guidance is in line with the statement published by the Financial Action Task Force (FATF) on 1 April 2020, encouraging Governments and Supervisory Authorities to work with Financial Institutions (FIs) and Designated Non-Financial Businesses and Professions (DNFBPs) in support of COVID-19 aid and containment efforts whilst remaining vigilant to new and emerging financial crime risks.

This Joint Guidance is issued pursuant to the Decree Federal Law No. (20) of 2018 on Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) and Illegal Organisations; and the powers vested, respectively, in:

- (i) Ministry of Justice and Ministry of Economy, both pursuant to Federal Law No. (1) of 1972 on the Jurisdictions of the Ministries and the Competence of the Ministers, including amendments thereto.
- (ii) the Central Bank of the UAE under the Central Bank Law, Decretal Federal Law No. (14) of 2018 Regarding the Central Bank & Organization of Financial Institutions and Activities (“Central Bank Law”);
- (iii) the Securities and Commodities Authority under Federal Law No. (4) of 2000 concerning the Emirates Securities and Commodities Authority and Market;
- (iv) the Insurance Authority, under Federal Law No. (6) of 2007 concerning the Establishment of the Insurance Authority & Organization of its Operations;
- (v) the Dubai Financial Services Authority pursuant to the Regulatory Law - DIFC Law No. (1) of 2004 concerning Dubai International Financial Centre;
- (vi) the Financial Services Regulatory Authority pursuant to Law No. (4) of 2013 concerning Abu Dhabi Global Market;



The Central Bank of the UAE (CBUAE), together with the Ministries of Justice and of Economy, the Securities and Commodities Authority (SCA), the Insurance Authority (IA), the Dubai Financial Services Authority (DFSA) of Dubai International Financial Centre (DIFC), the Financial Services Regulatory Authority (FSRA) of Abu Dhabi Global Market (ADGM) (collectively the “Supervisory Authorities”), believe that specific contextual guidance is needed. This Joint Guidance applies to all Financial Institutions (FI’s) and Designated Non-Financial Businesses and Professions (DNFBP’s) (where applicable) licensed, registered and regulated by the Supervisory Authorities.

While the United Arab Emirates (UAE) continues to implement precautionary measures to combat COVID-19, many FIs and DNFBPs may have changed the way in which they conduct business and interact with customers. For example, it may be more difficult for businesses to adhere to their existing customer identification and verification processes in seeking to meet customer due diligence obligations, particularly where institutions have adopted remote-working models.

The Supervisory Authorities recognise the challenges posed by the current situation and as such FIs and DNFBPs are expected to adapt their governance and operational processes to enable them to remain compliant with their regulatory obligations under the UAE Decree Federal Law on Anti-Money Laundering (AML) and Combating the Financing on Terrorism (CFT) and Illegal Organisations, its Implementing Regulation, Instructions, Guidelines, Notices, and Rules (‘AML Legislation’) issued by the Supervisory Authorities.

We remind FIs and DNFBPs that the mitigation of financial crime risk and effective control measures remains a key priority for the UAE. It is also important to be aware that in this challenging environment, FIs and DNFBPs should:

- remain vigilant as criminals may try to target their products and services;
- continue to manage money laundering and financing of terrorism risks effectively; and
- report suspicious transactions where required, to the UAE Financial Intelligence Unit (FIU).



مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.



ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

هيئة التأمين
Insurance Authority



UNITED ARAB EMIRATES
MINISTRY OF ECONOMY



UNITED ARAB EMIRATES
MINISTRY OF JUSTICE

هيئة الأوراق المالية والسلع
SECURITIES & COMMODITIES AUTHORITY



GENERAL GUIDANCE

Risk Assessments

The AML Legislation prescribes a risk-based approach to money laundering and terrorist financing risk that is commensurate with the institution's business, nature, size, and activities. Where the risk assessment process results in a lower risk rating, FIs and DNFBPs are granted the discretion to apply simplified due diligence measures. Equally, the COVID-19 circumstances introduce emerging risks that should dynamically be factored into FIs and DNFBPs' business and customer risk assessment and treatment of customers and transactions during this unprecedented time.

Customer Due Diligence

Customer On-Boarding

FIs and DNFBPs may be challenged to meet customers face-to-face given ongoing movement restrictions on non-essential travel. As a result, traditional methods to obtain and verify a customer's identity are being compromised and FIs and DNFBPs are urged to adopt alternate and non-traditional means to meet their obligations under AML Legislation. The Supervisory Authorities remind FIs and DNFBPs of the importance of continuing to meet the customer due diligence obligations in order to mitigate financial crime risk.

During this period, and in line with the FATF Standards, the UAE's Supervisory Authorities encourage the use of technology, including Fintech, Regtech and Suptech to the fullest extent possible. FIs and DNFBPs should also take into consideration the published [FATF Guidance on Digital ID](#), which highlights the benefits of trustworthy digital identity for improving the security, privacy, and convenience of identifying people remotely for both onboarding and conducting transactions while also mitigating money laundering and terrorist financing risks. Utilisation of UAE government supported solutions such as the validation gateway of the Federal Authority for Identity and Citizenship (ICA); or the UAE Pass, for Emirates ID's is reiterated during this time.

Where a FI or DNFBP is unable to make use of such technology, exception handling provisions acceptable by the Supervisory Authorities can be utilised. However, the Supervisory Authorities expect such businesses to maintain a record of when these provisions were legally vetted and invoked and for Senior Management to be aware of such events, as part of its' AML Risk Management framework. Senior



Management must put a corrective action plan in place to resolve issues related to invocation of exceptional provisions once business operations are back to normal. Furthermore, appropriate risk mitigation measures should be considered in instances where verification standards are not in line with the FIs and DNFBPs risk-based approach.

Accordingly, FIs and DNFBPs are expected to revisit their risk assessment and control frameworks and revise their internal policies, procedures, and/or control measures as necessary where such enhancements are warranted. In line with the provisions of Cabinet Decision No. (10) of 2019, concerning the Implementing Regulation of Decree Federal Law No. (20) of 2018 on AML and CFT and Illegal Organisations, Senior Management must formally approve and document policy and procedural amendments and any changes to current practices where revised measures have been adopted.

Non-Static Customer Identity Documentation

In relation to non-static customer identity documentation (e.g. passport number, residency visa expiry date etc.), the UAE Cabinet recently approved a package of new decisions to preserve health and safety, and to ensure the workflow and continuity of government work in various sectors. This includes measures to automate renewals of certain non-static customer identification documents. FIs and DNFBPs are expected to keep abreast of these developments and their impact on their AML and CFT systems and controls. FIs and DNFBPs should also engage with their customers to encourage utilization of government smart services to renew necessary identification documents and trade licenses through online channels.

Transaction Monitoring

Transaction Monitoring Systems

Circumstances prevailing as a result of the COVID-19 pandemic could lead to altered patterns of normal and suspicious transactional behavior. FIs and DNFBPs are advised to carefully analyse transactions to distinguish new patterns between those that are representative of suspicious behavior and those that are merely new normal patterns, and adjust their systems of monitoring and alerts to adopt new rules for reporting under exceptional social circumstances.



At this crucial point in time, FIs and DNFBPs should continue to apply a risk-based approach and closely monitor business relationships for criminal activities, due to the increase of financial fraud and exploitation scams, which could include the illicit fundraising for charitable causes without a government permit, and the perpetration of cybercrimes such as phishing schemes. It is likely that terrorists may also exploit these opportunities to raise funds. The FATF has issued a detailed paper on [COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses](#) which highlight key emerging risks and topics to be taken into account.

Supervisory Authorities expect FIs and DNFBPs to be mindful of their obligations to review the quality and timeliness of alerts generated from Transaction Monitoring Systems. Where reasonable grounds exist to suspect that a transaction, attempted transaction, or funds constitute criminal proceeds in whole or in part, or are related to a crime or are intended to be used in such activity, they are reminded to report the relevant transaction to the FIU without any delay. In this regard, Supervisory Authorities expect all FIs and DNFBPs to continue transactional monitoring operations in line with ongoing business activities.

Suspicious Transaction Reporting

The Supervisory Authorities expect all FIs and DNFBPs to report suspicious transactions and activities through the FIU's goAML reporting platform on a timely basis. Should FIs and DNFBPs encounter operational challenges in accessing goAML due to the COVID-19 situation, the FIU should be contacted at UAEFIU@cbae.gov.ae to make interim reporting arrangements. FIs and DNFBPs are reminded that a failure to report a suspicious transaction or activity, whether intentionally or by gross negligence, is a Federal Offence.

Sanction Screening Processes

FIs and DNFBPs are reminded of their obligations to update their records on a daily basis in order to identify individuals or entities designated by either the United Nations Security Council (UNSC) and/or the UAE Cabinet. Where an alert is generated, FIs and DNFBPs are required to conduct, without delay, a quality and timely review by cross-checking their customer databases against the generated alerts and maintaining the prerequisite recordkeeping requirements. FIs and DNFBPs are reminded that where a



مصرف الإمارات العربية المتحدة المركزي
CENTRAL BANK OF THE U.A.E.



ABU DHABI GLOBAL MARKET
سوق أبوظبي العالمي

هيئة التأمين
Insurance Authority



UNITED ARAB EMIRATES
MINISTRY OF ECONOMY



UNITED ARAB EMIRATES
MINISTRY OF JUSTICE

هيئة الأوراق المالية والسلع
SECURITIES & COMMODITIES AUTHORITY



match to a listing of an individual or entity to the relevant UNSC Sanctions lists or Local lists is identified, FIs and DNFBPs are required immediately and without delay to freeze the funds and notify their relevant supervisor. The same would apply for a delisting match.

If any further concerns arise or assistance is required, FIs and DNFBPs should contact their respective Supervisory Authority.