National Anti-Money Laundering and Combating Financing of Terrorism and Financing of Illegal Organizations Committee

United Arab Emirates

Joint Guidance on Combating the Use of Unlicensed Virtual Asset Providers in the United Arab Emirates

Supervisory Authority Sub-Committee

JOINT GUIDANCE ON COMBATING THE USE OF UNLICENSED VIRTUAL ASSET SERVICE PROVIDERS IN THE UNITED ARAB EMIRATES

The Joint Guidance provided in this document aligns with the Financial Action Task Force (FATF) publication on updated guidance for a risk-based approach to virtual assets and virtual asset service providers, particularly concerning the use and treatment of unlicensed virtual asset providers.

This Joint Guidance is issued pursuant to the Federal Decree No. 20 of 2018 on Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) and Illegal Organisations, as amended by Federal Decree No. 26 of 2021 (collectively known as the "AML legislation"); and the powers vested, respectively, in:

- 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");
- The Dubai Financial Services Authority pursuant to the Regulatory Law - DIFC Law No.9 of 2004 concerning Dubai International Financial Centre;
- The Financial Services Regulatory Authority pursuant to Law No. (4) of 2013 concerning Abu Dhabi Global Market;
- The Securities and Commodities Authority under Federal Law No. (4) of 2000 concerning the Emirates Securities and Commodities Authority and Market;
- 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;
- Dubai Law No. (4) of 2022, Regulating Virtual Assets in the Emirate of Dubai.

The Central Bank of the UAE (CBUAE), together with the Securities and Commodities Authority (SCA), the Virtual Assets Regulatory Authority (VARA), the Dubai Financial Services Authority (DFSA) of Dubai International Financial Centre (DIFC), the Financial Services Regulatory Authority (FSRA) of Abu Dhabi Global Market (ADGM), the Ministries of Justice and Economy (collectively the "Supervisory Authorities"), would like to educate the public on the risks associated with unlicensed virtual asset service providers (VASPs) given the recent developments taking place in the sector.

The global, cross-border nature, rapid development and evolution of virtual asset transfers, increasing functionality, and growing adoption of virtual assets makes it urgently important for the United Arab Emirates (UAE) to mitigate the money laundering, terrorist financing and proliferation financing risks presented by virtual asset activities.

While the UAE promotes a culture of innovation, investment and financial inclusion, it is essential for such activities to be conducted exclusively through channels with appropriate regulatory licences. As the use of virtual assets increases, the public is urged to confine their virtual asset transactions to licensed entities. This measure aims to protect the integrity of the UAE's financial sector, protect investors, safeguard licensed financial activities from unlawful competition, and prevent terrorism and proliferation financing, and the laundering of illicit proceeds within the UAE.

The Supervisory Authorities recognise the challenges faced by Licenced Financial Institutions (LFIs), Designated Non-Financial Businesses and Professions (DNFBPs) and Licenced Virtual Asset Service Providers (VASPs). Therefore, these licensed entities are expected to further enhance their governance and operational processes, and address such trends and emerging

risks. Licensed entities are reminded to comply with their regulatory obligations under the AML legislation, along with Regulations, Instructions, Guidelines, Notices, and Rules issued by the Supervisory Authorities.

LFIs, DNFBPs and VASPs are advised to further consult the FATF Report on Red Flag Indicators of Money Laundering and Terrorist Financing regarding Virtual Assets, as well as any other relevant Guidance/Reports published from other independent inter-governmental bodies and the Supervisory Authorities.

We remind LFIs, DNFBPs and VASPs that the mitigation of financial crime risk and effective control measures remains a key priority for the UAE, and hence they are expected to:

- Remain vigilant of the various fraudulent methods unlicensed VASPs adopt;
- Continue to manage money laundering, financing of terrorism and proliferation financing risks effectively;
- Ensure such emerging risks are factored into the LFIs, DNFBPs, and VASPs' business and customer risk assessments;
- Ensure adequate Due Diligence is conducted on VASPs to effectively identify instances where documents have been fabricated or forged, that may increase risks associated with money laundering, terrorist financing and/or proliferation financing;
- Identify instances whereby investors/customers are actively seeking or repeatedly utilising the services of unlicensed VASPs;
- Carefully analyse transactions to distinguish new high risk patterns and adjust their systems of monitoring and alerts to adopt new rules for reporting;
- Implement sufficient controls to effectively intercept transactions with unlicensed VASPs using advanced technologies;
- Report suspicious transactions and activity where required, to the UAE Financial Intelligence Unit (FIU); and
- Run awareness campaigns for their customers to educate investors how they can identify unlicensed entities and the associated risks.

Red Flags of unlicensed VASPs and other Guidance provided to LFIs, DNFBPs, VASPs and the general public:

The Supervisory Authorities have noted that suspicious parties are employing diverse and innovative ways and methods of inflicting upon their victims.

Among these methods, the most prominent ones are listed below, in a non-exhaustive manner:

- **Lack of regulatory license:** Unlicensed VASPs typically lack official licensing from Supervisory Authorities in the UAE and present themselves as licensed. It is crucial to inquire about the regulatory bodies overseeing the VASPs and verify this information via the respective Supervisory Authorities official website.
- **No physical presence:** Unlicensed VASPs may lack a physical presence, such as a registered office or a legitimate business address in the UAE.
- **Unrealistic promises/Ponzi schemes:** Beware of VASPs promising exceptionally high returns or guaranteed profits with minimal risk. They may be using funds from new investors to pay returns to earlier investors, creating an illusion of profitability.

- **Poor website and communications:** A poorly designed website, lack of contact information and unprofessional communication are warning signs.
- **Pressure to invest quickly:** Scammers may use high pressure tactics to rush consumers into making quick investment decisions.
- **Investments in unlicensed products (virtual assets):** Licensed VASPs are allowed to provide financial services and other activities licensed by the Supervisory Authorities virtual assets only. LFIs, DNFBPs, VASPs and customers are invited to find out more about these on the Supervisory Authorities' official website.
- **No consumer protection:** Unlicensed VASPs often do not provide adequate investor protections, such as safeguards on client assets (especially where custody/safekeeping services are provided), insurance coverage or an avenue for dispute resolution.
- **Lack of regulatory disclosure:** Unlicensed VASPs may not provide required disclosure, such as risk warnings or terms and conditions.
- **No record of compliance:** Research the Unlicensed VASP's history and verify if it has faced legal actions, regulatory fines, or consumer complaints. A lack of compliance with regulations is a red flag.
- **Unsolicited contact:** Be cautions of unsolicited communications or cold calls from unlicensed VASPs. Reputable companies typically do not engage in aggressive marketing tactics.
- **Social engineering:** Be aware of social engineering attacks (most notably phishing which involves fraudulent emails or websites that impersonate legitimate crypto exchange or wallets) when dealing with virtual assets.
- **Fraudulent ICO:** Beware of participating in Initial coin offering (ICO's) that have not been approved or registered by a Supervisory Authority. ICOs are fundraising methods where new cryptocurrencies are offered to the public. Fraudulent ICOs are those that promise revolutionary projects but failed to deliver, essentially stealing investors' funds.
- **Fake wallets and exchanges:** Scammers create fake cryptocurrency wallets or exchanges that appear legitimate (usually promising excessive returns in a short time frame). Users then deposit their assets onto these platforms, only to discover that their funds have been stolen.
- **Illicit user of virtual currency:** Transactions involving crypto asset exchanges which are followed within a short time by funds transfers to or ATM withdrawals in high risk geographies.
- **Illicit use of virtual currencies:** Purchase of crypto assets shortly following receipt of funds transfers from unconnected third parties.
- **Illicit use of virtual currency:** Multiple accounts are used to collect and funnel funds to a small number of crypto assets records.
- **Illicit use of virtual currency:** Repeated receipt of funds transfers from crypto asset exchanges, inconsistent with customer profile.
- **Purchase or sale of freehold property/real estate** where the funds used to carry out the transaction were converted from or to a virtual asset for a portion or the entire property value.
- **Purchase or sale of freehold property/real estate** where the method of payment is a virtual asset for a portion or the entire property value.
- **Terrorism financing:** Fundraising through virtual currencies**.**

- **Payment made via** virtually any method (cash, wire, cheque, bank drafts, etc.) **by a third party with no connection** to the underlying transaction.

Suspicious Transaction Reporting
The Supervisory Authorities expect all LFIs, DNFBPs, and VASPs to report suspicious transactions and activities through the FIU's goAML reporting platform in a timely manner. LFIs, DNFBPs, and VASPs are reminded that a failure to report a suspicious transaction or activity, whether intentionally or by gross negligence, is a federal offence.

Any information related to unlicensed virtual asset activities can be reported through whistleblowing mechanisms, to help regulatory authorities in their efforts to uphold the law and protect the UAE financial system.

The relevant regulatory authorities will actively investigate reports received through these mechanisms (email or phone call), while ensuring confidentiality and protection against retaliation.

Regulatory Authority	Contact Number	Email or Website
CBUAE	+971 (0)2 691 5555	https://eservices.centralbank.ae/wb/whistleblowing.html
SCA	+971 (0)2 627 888	good.governance@sca.ae
DFSA	+971 (0)4 362 1500	whistle@dfsa.ae
ADGM	+971 (0)2 333 8955	whistleblowing@adgm.com
VARA		https://www.vara.ae/en/register-a-complaint/

Civil and Criminal Penalties
VASPs operating in the UAE without a valid license will be subject to civil and criminal penalties including, but not limited to, financial sanctions against the entity, owners and senior managers. Furthermore, LFIs, DNFBPs, and VASPs which demonstrate wilful blindness in their dealings with unlicensed VASPs and have weak AML/CTF/CPF controls may be subject to enforcement action.

This public note serves as a reaffirmation of the UAE's commitment to promoting responsible innovation and maintaining the highest standards of financial integrity and national security. If any concerns arise or assistance is required, LFIs, DNFBPs and VASPs should contact their respective Supervisory Authority and the UAE's FIU.