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

ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM

GUIDANCE FOR LICENSED FINANCIAL INSTITUTIONS ON RISKS RELATED TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

20 February 2023

Contents

1. Introduction

1.1. Purpose

Article 44.13 of the *Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation of Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations* charges Supervisory Authorities with "providing Financial Institutions…with guidelines and feedback to enhance the effectiveness of implementation of the Crime-combatting measures."

The purpose of this Guidance is to **assist** the understanding and effective performance by the United Arab Emirates Central Bank's ("CBUAE") licensed financial institutions ("LFIs") of their statutory obligations under the legal and regulatory framework in force in the UAE, as detailed in section 1.3 below. It should be read in conjunction with the CBUAE's *Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations* (issued by Notice No. 74/2019 dated 19/06/2019) and *Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions* (issued by Notice 3090/2021dated 29/06/2021) and any amendments or updates thereof.[1] As such, while this Guidance neither constitutes additional legislation or regulation nor replaces or supersedes any legal or regulatory requirements or statutory obligations, it sets out the **expectations** of the CBUAE for LFIs to be able to demonstrate compliance with these requirements. In the event of a discrepancy between this Guidance and the legal or regulatory frameworks currently in force, the latter will prevail. This Guidance may be supplemented with additional separate guidance materials, circulars, and notices, and outreach sessions and thematic reviews conducted by the Central Bank.

Furthermore, this Guidance takes into account standards and guidance issued by the Financial Action Task Force ("FATF")[2], industry best practices, and red flag indicators. These are not exhaustive and do not set limitations on the measures to be taken by LFIs in order to meet their statutory obligations under the legal and regulatory framework currently in force. As such, LFIs and registered hawala providers ("RHP") should perform their own assessments of the manner in which they should meet their statutory obligations.

This Guidance comes into effect immediately upon its issuance by the CBUAE with LFIs expected to demonstrate compliance with its requirements within one month from its coming into effect.

1.2. Applicability

Unless otherwise noted, this Guidance applies to all natural and juridical persons, which are licensed and/or registered by the CBUAE, in the following categories:

[1] Available at: https://www.centralbank.ae/en/cbuae-amlcft.
[2] For example, please see: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html

- National banks, branches of foreign banks, exchange houses, finance companies, payment service providers, registered hawala providers; and
- Insurance companies, agencies, and brokers.

Multiple regulatory and supervisory agencies comprise the UAE's AML/CFT framework for virtual asset service providers ("VASPs"), including: the UAE Securities and Commodities Authority ("SCA"), which serves as the licensing and primary regulatory authority for VASPs at the Federal level and for the UAE's Commercial Free Zones ("CFZs"); the Virtual Asset Regulatory Authority ("VARA"), which serves as the regulator of VASPs in the Emirate of Dubai; the Financial Services Regulatory Authority ("FSRA"), which regulates VASPs in the Abu Dhabi Global Market ("ADGM"); the Dubai Financial Services Authority ("DFSA") which regulates VASPs in the Dubai International Financial Centre ("DIFC") and the CBUAE, which supervises LFIs and RHPs, including in their capacity as financial service providers to VASPs and to non-VASP customers that may engage in virtual asset ("VA") transactions. Additional detail on the UAE legal and regulatory framework for VASPs, including references to specific guidance issued by the aforementioned authorities, can be found in section 2.4 below. Prior to and during engagements with VASPs, LFIs and RHPs should consider the relevant jurisdiction and/or asset specific regulations mandated by the aforementioned supervisory agencies.

1.3. Legal Basis

This Guidance builds upon the provisions of the following laws and regulations:

(i) Federal Decree-Law No. (14) of 2018, Regarding the Central Bank & Organization of Financial Institutions and Activities, and its amendments ("CBUAE Law");

(ii) Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering ("AML") and Combatting the Financing of Terrorism ("CFT") and its amendments ("AML-CFT Law");

(iii) Law No. 4 of 2022 on the Regulation of Virtual Assets in the Emirate of Dubai;

(iv) Cabinet Decision No. (10) of 2019, as amended by Cabinet Decision No. (24) of 2022, Concerning the Implementing Regulation for Decree-Law No. (20) of 2018 on AML and CFT and Financing of Illegal Organisations ("AML-CFT Decision") and its amendments;

(v) Cabinet Decision No. (74) of 2020 Regarding Terrorism Lists Regulation and Implementation of United Nations Security Council (UNSC) Resolutions on the Suppression and Combating of Terrorism, Terrorist Financing, Countering the Proliferation of Weapons of Mass Destruction and its Financing and Relevant Resolution ("Cabinet Decision 74"), and its amendments;

(vi) Cabinet Decision No. (58) of 2020 regulating the Beneficial Owner Procedures ("Cabinet Decision 58");

(vii) Federal Decree-Law No. (34) of 2021 concerning the Fight against Rumours and Cybercrime;

(viii) Cabinet Decision No. (111) of 2022 on the Regulation of Virtual Asset Service Providers; and

(ix) Cabinet Decision No. (112) of 2022 regarding the Delegation of Some Competencies related to Virtual Asset.

1.4. Acronyms

Terms	Description
ADGM	Abu Dhabi Global Market
AML	Anti-money laundering
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer due diligence
CFT	Combating the financing of terrorism
CFZ	Commercial Free Zone
DeFi	Decentralized finance
DFSA	Dubai Financial Services Authority
DIFC	Dubai International Financial Centre
DNFBP	Designated non-financial business or profession
EDD	Enhanced due diligence
Executive Office	Executive Office for Control and Non-Proliferation
FATF	Financial Action Task Force
FI	Financial institution
FIU	Financial Intelligence Unit
FSRA	Financial Services Regulatory Authority
ICO	Initial coin offering
IT	Information technology
LFI	Licensed financial institution
ML	Money laundering
NFT	Non-fungible token
NOC	No-objection certificate
OTC	Over the counter
IP	Internet protocol
P2P	Peer-to-peer
PEP	Politically exposed person
PML	Professional money laundering
RHP	Registered hawala providers
SAR	Suspicious activity report

SCA	Securities and Commodities Authority
SEC	Securities and Exchange Commission
STR	Suspicious transaction report
SVF	Stored Value Facilities
TF	Terrorist financing
TFS	Targeted financial sanctions
UN	United Nations
UNSC	United Nations Security Council
UNSCR	UN Security Council Resolution
VA	Virtual asset
VARA	Virtual Asset Regulatory Authority
VASP	Virtual asset service provider
VPN	Virtual private network

1.5. Key Terminology and Definitions

This Guidance uses the following key terms and definitions, in alignment with the FATF definitions.

As defined in Article 1 of the AML-CFT Decision, as amended, a **virtual asset** is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes, excluding digital representations of fiat currencies, securities, and other funds (such as those separately regulated by the competent authorities of the UAE, including the CBUAE, SCA, VARA, FSRA, and the Dubai Financial Services Authority ("DFSA")). Virtual assets, so defined, typically include assets commonly referred to as cryptocurrencies, cryptocoins, payment tokens, exchange tokens, and convertible virtual currencies. Without prejudice to the definitions in the laws and regulations referred to above, stablecoins may be considered either virtual assets or traditional financial assets depending on their exact nature. No asset should be considered a virtual asset and a traditional financial asset (e.g., a security) at the same time.

Digital assets that are unique, rather than interchangeable, and that are in practice used as collectibles rather than as payment or investment instruments, are often referred to as **non-fungible tokens** ("NFTs") or crypto-collectibles. Such assets, depending on their characteristics, are generally not considered to be VAs for the purpose of this Guidance. However, it is important to consider the nature of the NFT and its function in practice, rather than what terminology or marketing terms are used. Some NFTs that on their face do not appear to constitute VAs may fall under the VA definition if they are used for payment or investment purposes in practice.[3] LFIs should determine as part of customer due diligence (section 4.2

[3] Similarly, NFTs that are fractionalized or issued as part of a large series or collection may be viewed by regulatory authorities in some jurisdictions as fungible shares of a larger financial asset and thus as subject to securities regulations.

below) whether a customer's proprietary NFT transactions fall under the VA definition and whether a customer's NFT-related business activities constitute covered VASP activities.

As defined in the AML-CFT Decision, as amended, a **virtual asset service provider** is any person—whether an individual or a company—that conducts any of the following five activities ("VASP activities" or "covered VASP activities") as a business on behalf of other individuals or companies. Note that the descriptions and examples of the five covered VASP activities presented below are provided for illustrative purposes only and are not intended to be comprehensive.

1. **Exchange between virtual assets and fiat currencies.** If parties can pay for VAs using fiat currency or can pay using VAs for fiat currency, the offerer or provider of this exchange service when acting as a business is a VASP.[4]
2. **Exchange between one or more forms of virtual assets.** If parties can use one kind of VA as means of exchange or form of payment for another VA, the offerer or provider of this service when acting as a business is a VASP.
3. **Transfer[5] of virtual assets.** This activity type is meant to cover any service allowing users to transfer ownership, or control of a VA to another user or to transfer VAs between VA addresses or accounts held by the same user. If a new party has custody or ownership of the VA, has the ability to pass control of the VA to others, or has the ability to benefit from its use, then transfer has likely occurred. An example of a service covered this activity type is the function of actively facilitating or allowing users to send VAs to other individuals, as in a personal remittance payment, payment for nonfinancial goods or services, or payment of wages. A provider offering such a service will likely be a VASP.

[4] FIs or card service providers that simply provide the funding mechanism for the fiat side of an exchange transaction but do not conduct the exchange activity themselves are not considered to be engaging in the covered activity of "exchange between virtual assets and fiat currencies."
[5] In the context of virtual assets, **transfer** means to conduct a transaction on behalf of another natural or legal person that moves a virtual asset from one VA address or account to another.

Exchange and Transfer Services and Business Models

A range of common VA services or business models may constitute VASP activity types (1) through (3) for the purposes of this Guidance (hereafter referred to as "exchange and transfer activities"), including:

- **VA escrow services**, including services involving smart contract technology, that VA buyers use to send, receive or transfer fiat currency in exchange for VAs, when the entity providing the service has custody over the funds;
- **Brokerage services** that facilitate the issuance and trading of VAs on behalf of a natural or legal person's users;
- **Order-book exchange services**, which bring together orders for buyers and sellers, typically by enabling users to find counterparties, discover prices, and trade, potentially through the use of a matching engine that matches the buy and sell orders from users. However, a platform which only allows buyers and sellers of VAs to find each other and does not undertake any of the services in the definition of a VASP would not be a VASP; and
- **Advanced trading services**, which may allow users to access more sophisticated trading techniques, such as trading on margin or algorithm-based trading.

Exchange and transfer activities may also occur through technology commonly referred to as **decentralized exchanges or platforms**. A decentralized finance ("DeFi") application (i.e., the software program) is not itself a VASP. However, creators, owners, and operators who maintain control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralized, may fall under the definition of a VASP where they are providing or actively facilitating VASP services. For example, there may be control or sufficient influence over assets or over aspects of the service's protocol, and the existence of an ongoing business relationship between themselves and users, even if this is exercised through a smart contract or in some cases voting protocols.

Note, finally, that a VASP does not have to provide *every* element of the exchange or transfer in order to qualify as a VASP, so long as it conducts the exchange activity as a business on behalf of another natural or legal person.

4. **Safekeeping or administration of virtual assets or instruments enabling control of virtual assets.** Any entity that has the ability to exercise control over VAs may qualify as a VASP, including entities that provide the service of holding a VA or the private keys to the VA on behalf of another person, as well as the service of managing VAs for or on behalf of another person. This VASP activity type would include, for example, most custodial wallet service providers because they hold and/or keep VAs on behalf of another person. Note that "control" does not have to be unilateral and can include circumstances in which keys or credentials held by others are required in order to change the assets disposition, such as multi-signature processes.

5. **Participation in and provision of financial services related to an issuer's offer or sale of a virtual asset.** This VASP activity type covers persons who participate in, or provide related financial services to, issuers' offer and/or sale of VAs through activities such as initial coin offerings ("ICOs"). Such persons may be affiliated or unaffiliated with the issuer undertaking the ICO in the context of the issuance, offer, sale, distribution, ongoing market circulation and trading of a VA. For example, this could include businesses accepting purchase orders and funds and purchasing VAs from an issuer to resell and distribute the funds or assets, as well as book building, underwriting, market making and placement agent activity, etc.

VASP activities are not mutually exclusive, and a VASP may engage in one or more of these activities. Moreover, VASP activities are subject to AML/CFT regulations regardless of the type of VA involved in the financial activity, the underlying technology used, or the additional services that the platform potentially incorporates (such as a mixer or tumbler or other potential features for obfuscation). Please see section 2.2 below for a discussion of the primary VASP business models operating in the UAE and their associated money laundering ("ML")/terrorist financing ("TF") vulnerabilities, as well as Annex A for a more general overview of VASP services and business models.

This Guidance limits the definition of VASP to those entities that serve customers—that is, provides listed services *as a business* and *for or on behalf of another natural or legal person*, as stipulated in Article 1 of the AML-CFT Law, as amended. The phrase "as a business" is meant to exclude those who may carry out an otherwise covered VASP activity on a very infrequent basis for non-commercial reasons from coverage as VASPs The phrase "for or on behalf of another natural or legal person" includes carrying out of the function in the course of providing a covered service to another person. This person for whom or on whose behalf financial services may be conducted may also be referred to as a "user" or "customer" of those services. This means, for example, that an internal transfer of VAs by a single legal person within that legal person (that is, within units of a particular company for example) would not qualify as a VASP, unless that transfer was for or on behalf of another person in the context of providing VASP services.

The acceptance of VAs as payment for goods and services does not constitute a VASP activity. A service that facilitates companies accepting VA as payment would, however, be a VASP.

Finally, note that the CBUAE does not accept or acknowledge virtual assets as a legal tender/currency in the UAE; rather, the only legal tender in the UAE is the UAE dirham.[6] **As such, those accepting VAs as payment for goods and services or in exchange for other assets bear any risk associated with the future acceptance or recognition of VAs.**[7] As by definition VAs cannot be digital representations of fiat currencies, securities, or other separately regulated financial assets, a bank record maintained in digital format, for instance, that represents a person's ownership of fiat currency is not a VA. However, a digital asset that is exchangeable for another asset, such as a stablecoin that is designed to be exchangeable for a fiat currency or a VA at a fixed rate, could still qualify as a VA, depending on the relevant features of such a stablecoin. Under the definition provided above, a digital asset that has inherent value to be traded or

[6] See Articles 55-56 of the CBUAE Law.
[7] See "CBUAE re-iterates the objective of the new Stored Value Facilities (SVF) Regulation," available at: https://www.centralbank.ae/media/4ibgkhmc/cbuae-re-iterates-the-objective-of-the-new-stored-value-facilities-svf-regulation-en.pdf.

transferred and used for payment or investment is likely to qualify as a VA, whereas a digital asset that is simply a means of recording or representing ownership in something else is likely not to qualify as a VA.

Section 2.4 below provides an overview of the UAE's AML/CFT regulatory and supervisory framework for VASPs and VA-related activities, including a description of which virtual asset types and/or VASP activities fall within the purview of which competent authorities.

2. Understanding ML/TF Risks Related to VAs and VASPs

2.1. Threats Related to VAs and VASPs

Virtual assets, like more traditional forms of value such as cash and e-money, can be used to move or store value related to any kind of illicit activity, from fraud to the proliferation of weapons of mass destruction. In practice, however, VAs are more likely to be involved in certain types of illicit activity or in activities carried out by certain illicit actors. A survey of case studies contributed by FATF member jurisdictions found that use of virtual assets was most common in cases involving the illicit sale of narcotics and other controlled goods, such as firearms. Cases involving computer-based fraud and extortion were the second-most frequent.[8] Leading jurisdictional authorities have also linked virtual assets with drug trafficking and with cybercrimes such as ransomware attacks,[9] as well as arms-length criminal transactions in which the parties want to maintain a high degree of anonymity, such as purchases from online "dark web" marketplaces.[10]

Supervisory authorities in the UAE have also identified through engagement with the UAE Financial Intelligence Unit ("FIU") and the private sector the existence of professional money laundering ("PML") schemes that allow criminals to cash out proceeds generated in virtual currency via illicit online markets (e.g., Dark Web drug-trafficking marketplaces).

An infographic on a UAE specific typology can be found in Annexure C.[11]

Retail investors and other users of virtual assets should be aware that virtual asset markets, as they are currently operating, offer less consumer protection than traditional financial markets, with correspondingly greater risks of fraud and manipulation. Key consumer and investor risks include:

- **Hacks.** Virtual assets may be targets for hackers, who have been able to breach sophisticated security systems in order to steal funds.

[8] FATF, *Virtual Assets Red Flag Indicators of Money Laundering And Terrorist Financing*, September 2020, p. 4, https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf.
[9] *U.S. National Money Laundering Risk Assessment*, 2018, p. 3, https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf.
[10] HM Treasury, *National risk assessment of money laundering and terrorist financing 2020*, December 2020, p. 71, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf.
[11] Supervisory Authorities Sub-Committee and UAE Financial Intelligent Unity, *Typologies in the Financial Sector*, September 2021, p. 9. See also Federal Bureau of Investigation, "FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic," https://www.fbi.gov/news/pressrel/press-releases/fbi-expects-a-rise-in-scams-involving-cryptocurrency-related-to-the-covid-19-pandemic.

- **Fewer protections.** If you trust a company to hold your virtual assets and something goes wrong, that company may not offer you the kind of help you expect from a bank or debit or credit card provider.
- **Cost.** Virtual assets can cost more to use than credit cards or even regular cash once you take exchange rates and fees into consideration.
- **Scams.** Fraudsters have been known to take advantage of the hype surrounding virtual assets to cheat people with fake opportunities. Virtual asset companies offering "guaranteed" investment returns or promises of high returns for little risk should be viewed sceptically.

2.2. Vulnerabilities of VAs and VASPs

Virtual assets in general are a high-risk medium of exchange, but the level of vulnerability to abuse for illicit activity is not identical across virtual asset types. Cryptocurrencies, the most common form of virtual assets, are most vulnerable to abuse because they have inherent characteristics that illicit actors can exploit:

- **Decentralization.** Many cryptocurrencies facilitate peer-to-peer financial transactions without the involvement of any intermediaries. The exclusion of third parties subject to financial laws, regulations, or pressure from governments enables illicit actors to use cryptocurrencies to purchase goods and services without regulatory oversight—despite the public visibility of these transactions on the blockchain.
- **Anonymity or pseudo-anonymity.** The structure and design of the cryptocurrency economy makes it possible for a virtual asset owner to avoid any interactions that would require the virtual asset owner to reveal his or her true identity, although transactions registered on the blockchain typically include other non-personal identifiers such as wallet addresses. Major players in the cryptocurrency economy can preserve a high degree of anonymity through the design and delivery of their products and services. Parties transacting on the blockchain do not need to trust, or even know, each other before they can do business, and certain cryptocurrencies, often called "privacy coins," further enhance anonymity. As a result, in many instances a participant in this sector is only forced to reveal his or her true identity when converting between virtual assets and fiat currencies.

  Lack of customer and counterparty identification is especially concerning given the cross-border nature of VAs and the inadequate or uneven regulation and supervision of VA activities and providers across jurisdictions, as described below.

  - **Anonymizing Services:** Beyond the degree of anonymity or pseudo-anonymity afforded by the inherent features of most virtual assets, there exist anonymizing services that specialize in anonymizing cryptocurrency transactions on the blockchain. Many blockchains are entirely public—which means all transactions to and from a particular wallet are open to public scrutiny. Anonymizing services, also known as mixers or tumblers, thwart such analysis, using tactics such as distributing the assets to thousands of accounts and then re-aggregating them and sending them back to their original owners, or onward

to their ultimate recipient, functioning in a manner similar to the layering phase of money laundering. Such services are particularly useful to criminals or terrorist financiers who seek to evade analysis of their activities by law enforcement authorities.

These characteristics are similar to cash in that they allow transactions to take place with minimal involvement by third parties—with these risks heightened further given the non-face-to-face nature of VA transfers and the technical complexity of the underlying blockchain infrastructure, which can inhibit effective monitoring and risk management by third parties or VASPs that lack a sophisticated understanding of the business models, threats, and vulnerabilities associated with VAs.

VAs have certain additional features, however, that make them more practical than cash as a medium of global commerce. Perhaps most importantly, they allow counterparties to conduct an exchange of value without ever being in the same place, and they are equally valid in any jurisdiction. This use case is supported by additional features of this asset type:

- **Immutability.** Transactions on the blockchain are largely irreversible, making it very difficult—if not impossible—to recover missent, hacked, or stolen funds, particularly without the cooperation of a reputable VASP involved in the transaction chain. Several high-profile hacks of VASPs over the years highlight this risk.
- **Large Transactions and High Frequencies.** It is simple to conduct high-value and high-velocity virtual asset transactions with relatively little scrutiny or inconvenience. A Bitcoin transaction worth USD 100 million can be confirmed and validated on the blockchain in roughly 10 minutes without any regulatory agency or law enforcement inquiries. In comparison, moving USD 100 million gained illicitly through the traditional financial system would require creating an intricate and highly complex international money laundering operation over several years. It would also be challenging for a criminal organization to physically move USD 100 million in fiat notes due to the massive weight of such an amount. In contrast, a USB flash drive containing the private keys to a Bitcoin wallet with USD 100 million in Bitcoin can easily fit into a pocket.

Not all virtual assets share these same characteristics and risks, however. Some cryptocurrencies and other types of virtual assets use a blockchain but rely on a centralized authority that asserts control over participation in the network and access to the blockchain, including by conducting customer due diligence on key participants. However, cryptocurrencies with all of the above risk attributes continue to be the most popular and most traded form of virtual assets.

As vehicles for virtual assets, VASPs have elevated illicit finance vulnerabilities that are similar to those of FIs that bank cash-based businesses. By contrast, LFI relationships with VASPs have elevated illicit finance vulnerabilities that are similar to those posed by correspondent relationships, due to the intermediating role played by the VASP customer, which facilitates activity between the LFI and a third party. The fact that VASPs in many jurisdictions are subject to little or no regulatory oversight or ineffective regulatory oversight provides additional vulnerabilities that illicit financial actors can exploit:

- **Weak Regulatory and Supervisory Architecture.** Virtual assets and VASPs have developed and attained public adoption faster than regulatory coverage has evolved; most jurisdictions are struggling to understand and effectively regulate the sector. The existence of unregulated VASPs raises risk across the sector, and the newness of jurisdictions' regulatory regimes for VASPs means banks cannot assume that VASPs—even those in jurisdictions with relatively mature regulatory regimes—are subject to effective oversight.
- **Insufficient Preventive Measures.** VASPs—particularly those operating in jurisdictions with weak or nonexistent regulatory frameworks—often have poorly developed preventive and risk mitigation measures. Even many VASPs in jurisdictions with stronger or more mature regulatory regimes are new businesses that lack experienced compliance staff and/or have insufficient compliance budgets. Finally, some people involved with the operation of VASPs are ideologically opposed to government intervention and look to virtual assets as a privacy-focused alternative to the traditional financial sector, making them reluctant to impose preventive and mitigating measures they perceive as excessive, despite being requirements under international AML/CFT standards.

VASPs can operate using a variety of different business models that present different levels of vulnerability based on the characteristics of the product and service offerings on which they focus. Many VASPs operating in the UAE appear to fall into one of three main business models:

- **Trading Exchanges:** Several VASPs currently operational in the UAE are licensed to operate as multilateral trading facilities[12] and to provide exchange and custodial services to both retail and institutional investors. Such firms facilitate the exchange of fiat currency for approved virtual assets, as well as the exchange of approved virtual assets for other approved virtual assets. Exchanges are key elements of the virtual asset sector because they offer fiat "on" and "off ramps" (the opportunity to exchange fiat currencies for virtual assets) and high liquidity. They are potentially vulnerable to abuse by illicit actors, who may seek to "clean" virtual assets associated with a criminal wallet by transferring the value to a new blockchain. As such, they can be key nodes for crimes involving virtual assets.
- **Over the Counter ("OTC") Brokers:** A number of entities and individuals advertise themselves as operating in the UAE and providing OTC brokerage services. OTC brokerage involves direct, discretionary facilitation of virtual asset sales and purchases between individual buyers and sellers who cannot or do not want to transact on an open exchange. These transactions usually involve large quantities of virtual assets and involve institutional investors or other major virtual asset investors. OTC brokerage offers many of the same advantages as exchanges but often handle far larger transactions than are permitted on such exchanges. Internationally, OTC brokers may trade with markets or exchanges that are not adequately regulated, and OTC brokers themselves often have less stringent know-your customer requirements than the exchanges through which they

[12] Multilateral Trading Facilities are specifically defined and regulated in ADGM by the FSRA. According to the FSRA's Guidance on the Regulation of Digital Securities Activities in ADGM (24 February 2020), "Market intermediaries (e.g., broker dealers, custodians, asset managers) dealing in or managing Virtual Assets, and Multilateral Trading Facilities using Virtual Assets, need to be licensed / approved by FSRA. Only activities in Accepted Virtual Assets will be permitted."

transact, making them comparatively attractive to illicit actors who wish to launder large sums. Moreover, OTC brokers are currently not licensed or authorized by or subject to the regulations of any UAE authority, and as such, their customers receive no protection under existing financial services regulations unless licensed or authorized.

- **Virtual Asset Transmission**: A few entities advertise themselves as providing virtual asset transmission services, sending virtual assets to a designated wallet in return for cash. These entities also generally conduct exchange on a small scale, accepting payment to purchase virtual assets on the customer's behalf from a larger exchange. This business model is very vulnerable to abuse by illicit actors, as unlike trading exchanges or OTC brokers it allows customers to exchange cash for virtual assets. In addition, transactions carried out by the business on behalf of a customer will appear to be made only by the business itself, thwarting surveillance of transactions on the blockchain.

Please see Annex A for a description of additional VASP services and business models. As noted above, these descriptions and examples of VASP activities and business models are provided for illustrative purposes only and are not intended to be comprehensive.

2.3. LFIs' Potential Exposure to VAs and VASPs

LFIs may face exposure to VAs and VASPs through relationships or transactions with the following:

- **Direct services to VASP customers:** LFIs' most direct means of exposure to VA or VASP activity is through customer relationships with VASPs.
    - Under Article 33 bis 1 of the AML-CFT Decision, as amended, every natural or legal person who carries out any VASP activities, provides VASP products or services, or carries our VASP operations from the state must be licensed, enrolled, or registered by a competent supervisory authority in the UAE. As such, **LFIs are strictly prohibited from establishing relationships or processing transactions with individuals or entities that perform covered VASP activities and are not licensed to do so by UAE authorities.** It is therefore essential that LFIs form an understanding of whether its customers perform covered VASP activities and, if so, whether they have fulfilled applicable UAE licensing requirements. **LFIs are not permitted to establish relationships or process transactions with foreign VASPs that have not secured a license to operate as a VASP from UAE authorities, even if the foreign VASP is duly licensed or registered outside the UAE.**

  Additional detail regarding the UAE legal and regulatory framework for VASPs is provided in section 2.4 below. See section 4.2.1.3 for guidance on determining whether a customer qualifies as a VASP and is therefore subject to additional specific and/or enhanced due diligence measures. Specific due diligence measures for all VASP customers, regardless of risk, are detailed in section 4.2.2 below, and EDD measures for VASP customers determined to pose higher risks are detailed in section 4.2.3.1.

- **Downstream services to third-party (i.e., non-customer) VASPs:** Additionally, LFIs may be indirectly exposed to VA or VASP activity through its customers that use their account or relationship with the LFI to provide downstream financial services to VASPs. In the case of VASP customers, this may include the provision of accounts or custodial wallets that can be used directly by customers of a third-party VASP to transact business on the customer's own behalf.

  EDD measures for VASP customers that transact or maintain relationships with third-party VASPs are detailed in section 4.2.3.1 below.

- **Services to other customers that transact in VAs:** LFIs may be exposed to VA or VASP activity through customers (other than FIs or VASPs) that use their accounts or relationships with the LFI to conduct virtual asset exchange transactions on their own behalf through a VASP or directly with other individuals or entities. LFIs may observe such activity in the form of *debits from* a customer's account to a VASP or other counterparty (for purposes of exchanging fiat currency for virtual assets) or *credits to* a customer's account from a VASP or other counterparty (for purposes of exchanging virtual assets into fiat currency). Note that, where a customer transacts with a VASP using a third-party payment processing service, the credit or debit will appear as a transfer to or from the third-party payment processor, rather than to or from the VASP itself.

  Customers that conduct a high volume or value of virtual asset exchange transactions may warrant the application of enhanced ongoing monitoring measures, as detailed in section 4.2.3.2 below.

- **LFIs' proprietary investments in VAs:** LFIs may also be exposed to risks associated with VAs and VASPs through their own, proprietary investment activity in the virtual asset market. LFIs should apply AML/CFT due diligence regarding any prospective VA investment target as well as any VASPs involved in facilitating such investments. Such measures are discussed in section 5 below.

2.4. UAE Legal and Regulatory Framework for VASPs

The AML-CFT Law brings virtual assets and virtual asset service providers within the scope of the UAE's AML/CFT legal, regulatory, and supervisory framework. Under Articles 9 and 15 of the AML-CFT Law, VASPs must report suspicious transactions and information relevant to such transactions to the UAE FIU, and under Articles 13 and 14, supervisory authorities are authorized to assess the risks of VASPs, conduct supervisory operations (including inspections) of VASPs, and impose administrative penalties on VASPs for violations of applicable laws and regulations. Additionally, the AML-CFT Law prohibits any natural or legal person to practise VASP activities without a license, entry, or registration, as applicable, from competent supervisory authorities.[13]

[13] See also Cabinet Decision No. 111 of 2022 on the Regulation of Virtual Asset Service Providers.

2.4.1. *SCA*

The SCA regulates platforms that enable the trading of virtual assets, authorized persons that carry out virtual asset custody services, and virtual asset intermediaries. The SCA defines virtual assets as digital representation of value that can be digitally traded or transferred and can be used for investment purposes and does not include digital representations of fiat currency, securities, or other money. A virtual asset, so defined, is neither issued nor guaranteed by any sovereign state or jurisdiction and fulfils the above functions only by agreement within the community of users of the virtual asset. A full description of regulated activities in relation to virtual assets and virtual asset service providers is provided in Cabinet Resolution No. (111) of 2022 on the Regulation of Virtual Asset Service Providers.

2.4.2. *CBUAE*

The CBUAE licenses **Payment Token Service Providers** pursuant to the Central Bank's Retail Payment Services and Card Schemes Regulation.[14] Under this regulation, Payment Tokens are defined as a type of Crypto-Asset that is backed by one or more Fiat Currency, can be digitally traded, and functions as a medium of exchange and/or a unit of account and/or a store of value, but does not have legal tender status in any jurisdiction. A Payment Token is neither issued nor guaranteed by any jurisdiction and fulfils the above functions only by agreement within the community of users of the Payment Token.[15] Payment Token Service Providers, in turn, are defined as persons engaged in Payment Token issuing, Payment Token buying, Payment Token selling, facilitating the exchange of Payment Tokens, enabling payments to Merchants and/or enabling peer-to-peer payments, and Custodian Services related to Payment Tokens.

Additionally, under the Stored Values Facilities ("SVF") Regulation of 2020 (Circular No. 6/2020),[16] the CBUAE licenses and supervises providers of SVFs, defined as facilities (other than cash) used by a customer to store money or "Money's Worth" and transfer such money or "Money's Worth" as a means of payment.[17] Under the SVF Regulation, "Money's Worth" includes "other forms of monetary consideration or assets such as values, reward points, Crypto-Assets, or Virtual Assets." To the extent that providers of SVFs engage in the VA exchange or transfer activities or other VASP activities, as described in section 1.5 above—including by facilitating companies accepting VA as payment[18]—they fall under the definition of a VASP and must be licensed to operate as such by UAE authorities.

2.4.3. *VARA*

Under Law No. 4 of 2022 on the Regulation of Virtual Assets in the Emirate of Dubai, a virtual asset is defined as a digital representation of value that can be digitally traded, transferred, or used as an exchange or payment tool or for investment purposes, and any digital representation of any other value as determined

[14] Available at:https://www.centralbank.ae/media/4came3rh/2021-c-15-2021-retail-payment-services-and-card-schemes-reg_0.pdf.
[15] See Retail Payment Services and Card Schemes Regulation, par. 73.
[16] Available at:https://www.centralbank.ae/media/pxzjtgdm/stored-value-facilities-svf-regulation-ar-en.pdf.
[17] Please consult the SVF Regulation for a complete definition of an SVF and related terms.
[18] See, e.g., FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, 2021, p. 32, available at: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Updated-Guidance-VA-VASP.pdf.

by VARA. Virtual assets, so defined, include "virtual tokens," defined as digital representations of a set of rights that can be digitally issued and traded through a virtual asset platform.[19] VARA, within the scope of the above-mentioned law and Cabinet Decision No. (112) of 2022, and without prejudice to the regulatory powers of the CBUAE and SCA, serves as the regulatory authority for VAs in the Emirate of Dubai responsible for authorizing any entity to undertake VA-related activities, including specifically licensing VASPs to carry out activities related to VAs.

VASPs are defined by this Law as any person authorised by VARA to conduct any activities that require a license from VARA and are subject to VARA oversight, per Article 16 of Law No. 4 of 2022.

2.4.4. *FSRA*

ADGM's regulatory framework for the regulation of virtual asset activities officially came into practice in 2018. The FSRA regulates platforms that enable the trading of virtual assets as multilateral trading facilities, authorised persons that carry out virtual asset custody services, and virtual asset intermediaries, including custodians, brokers, asset managers, and advisors. The FSRA defines virtual assets as digital representations of value that can be digitally traded and function as (i) a medium of exchange and/or (ii) a unit of account and/or (iii) a store of value, but that does not have legal tender status in any jurisdiction. A virtual asset, so defined, is neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual asset. As such, a virtual asset is distinguished from fiat currency (defined as government-issued currency that is designated as legal tender in its country of issuance through government decree, regulation, or law) and e-money (defined as a digital representation of fiat currency used to electronically transfer value denominated in fiat currency). A full description of regulated activity in relation to virtual assets is provided in the FSRA's document *Guidance – Regulation of Virtual Asset Activities in ADGM*.[20]

The FSRA considers e-money activities to be covered by its payments regulatory framework and separately defines and regulates "digital securities" under its Financial Services and Markets Regulations of 2015.[21]

2.4.5. *Other VASP Business Models*

In addition to understanding the risks associated with VASPs licensed under the UAE legal framework, LFIs and RHPs should also be aware of the vulnerabilities associated with other VASP business models and product features, as the VASP operating environment is rapidly evolving and subject to new entrants and changes in existing business models.

An overview of the vulnerabilities associated with other VASP business models is included as Annex A below.

---

[19] See https://dlp.dubai.gov.ae/Legislation%20Reference/2022/Law%20No.%20(4)%20of%202022%20Regulating%20Virtual%20Assets.html.

[20] See https://www.adgm.com/documents/legal-framework/guidance-and-policy/fsra/guidance-on-regulation-of-virtual-asset-activities-in-adgm.pdf?la=en&hash=2E446E61E82CB1252B499B56B485396D.

[21] See https://en.adgm.thomsonreuters.com/sites/default/files/net_file_store/ADGM1547_12483_VER122021.pdf.

3. Requirements for CBUAE's Non-Objection for Opening New Accounts for VASPs

3.1. Administrative Accounts

LFIs may establish operational accounts for VASPs (for example staff and administrative expense accounts and accounts for revenue from services rendered) without submitting a request for non-objection to the CBUAE.

3.2. Transactional Accounts

LFIs may establish transactional accounts for VASPs, i.e., accounts to be opened to hold client funds, on condition that any such account is a suitably protected escrow account that satisfies the following conditions:

a. Clients should deposit funds directly into the escrow account;

b. The LFI may allow either individual accounts (i.e., one per client) or a pooled account for deposits by all clients of the VASP;

c. Funds in the escrow account should be ring-fenced against withdrawals for any purpose other than payment as requested explicitly and exclusively by the VASP client;

d. Escrow accounts should be reconciled by the VASP on a daily basis, and the VASP should maintain the records for individual balances;

e. The LFI maintaining the escrow account should only be authorized to move funds for purposes of settlement, refund, etc.; and

f. The external auditor of a VASP should be required to review the escrow account on a monthly basis (based on an 'Agreed Upon Procedure') and report the deviations to its senior management for appropriate corrective action.

3.3. Jurisdiction

In case of disputes, the UAE courts should have jurisdiction over all transactions involving the UAE dirham.

3.4. Control Assurance

The LFI should ensure that controls (including the conditions stated above) are in place through formal written agreements and internally via stated policy, to mitigate any potential reputational risk, or risk of loss to the LFI, from such arrangements.

3.5. Non-Objection Process

LFIs should submit a request to the Central Bank for non-objection to open accounts for each VASP on a case-by-case basis. The request should include an attestation from the LFI's compliance department that the appropriate risk management controls required by the CBUAE have been fulfilled.

4. Mitigating ML/TF Risks Related to VASP Customers and VA-Related Customer Transactions

Effective risk mitigation is critical to protecting the LFI/RHP, complying with its legal obligations, and meeting supervisory expectations. When establishing and maintaining relationships with VASPs, entities that provide services to VASPs, or other customers engaging in VA transactions, LFIs and RHPs should establish and implement effective policies, procedures, and processes to identify higher-risk relationships, assess the AML/CFT risks of VASP or VA-exposed customers, conduct due diligence at account opening and throughout the relationship, and monitor these relationships for unusual or potentially suspicious activity. Effective, risk-based measures should be based on a sound, up-to-date understanding of the risks posed to LFIs and RHPs by VASPs and VA activity.

The sections below discuss how LFIs and RHPs can apply specific preventive measures to identify, assess, manage, and mitigate the risks associated with VASPs and VA activity. The controls discussed below should be integrated into the LFI's/RHP's larger AML/CFT compliance program and supported with appropriate governance and training.

Section 5 addresses controls that LFIs should put in place to mitigate the risks associated with any proprietary investments in VAs undertaken by the LFI itself.

4.1. Risk-Based Approach

Under article 4 of the AML-CFT Decision, any LFI is required to identify, assess and understand its ML/TF risks. For this purpose, LFIs must perform, document, and keep up to date an enterprise-wide risk assessment that includes an assessment of risks related to VASP or VA-exposed customers. An LFI's risk assessment should take into account all of the risk factors relevant to VASPs and VA activities, including those arising in relation to its:

- Customers, including those that operate as licenced VASPs, entities that provide services to VASPs, and other customers engaging in VA transactions;
- Products and services, including services that allow third-party VASPs to transact through the account or relationship with the LFI;
- Delivery channels, including non-face-to-face business relationships or transactions; and

- Geographies, including the jurisdictions or regions in which its VASP and VA-exposed customers are located or do business.

As part of the process of updating their enterprise-wide risk assessments, LFIs should perform a **one-time review and assessment of their existing customer portfolio** to understand if:

- Any existing customers meet the definition of a VASP, as set forth in section 1.5 above; or
- Any existing customers (other than FIs or VASPs) engage in:
    - High-volume or high-value VA transactions; and/or
    - Transactions with foreign VASPs located in high-risk jurisdictions.

LFIs should then establish a **compliance monitoring plan** for all such customers identified through the one-time portfolio review to ensure that the LFI refreshes the customer's risk profile and applies, where applicable, the specific and enhanced due diligence measures detailed in sections 4.2.2 and 4.2.3 below. **Where an LFI identifies an existing customer that meets the definition of a VASP but does not currently have a valid license to operate in the UAE—or where the customer's license to operate as a VASP has lapsed or been revoked or suspended—the LFI should restrict all transaction activity with or through the LFI until the customer has obtained the license, or a non-objection certificate ("NOC") addressed to the LFI for the VASP to open or continue operating a client money account, from applicable UAE authorities and has provided a copy of the license or NOC to the LFI.**

The LFI is expected to document the methodology and findings of the risk assessment, considering all relevant risk factors and assessing the design and effectiveness of its risk mitigation policies, procedures, systems, and controls. LFIs should keep their risks assessments up to date and ensure that identified risks are within the institution's risk appetite and that identified deficiencies are appropriately tracked and remediated. Risk assessments should provide a consolidated assessment of the LFI's ML/TF risks across all business units, product lines, and delivery channels, including those of branches, subsidiaries, parent entities, or other affiliates located outside the UAE.

ML/TF threats and vulnerabilities related to VAs and VASPs can be found in sections 2.1 and 2.2 above. For more details and information on the institutional risk assessment process, please consult the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 4.[22]

4.2. Customer Due Diligence

4.2.1. *General CDD Measures*

Customer due diligence ("CDD"), and where necessary enhanced due diligence ("EDD"), are the core preventive measures that help LFIs manage the risks of all customers, particularly higher-risk customers. Under Article 5 of AML-CFT Decision, LFIs must conduct CDD before or during the establishment of the business relationship or account, or before executing a transaction for a customer with whom there is no

[22] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

business relationship. LFIs should consult the UAE legal and regulatory framework currently in force and related CBUAE Guidance for a full discussion of their CDD obligations and of the CBUAE's expectations for CDD procedures. Consistent with local regulatory requirements, all LFIs must ensure compliance, where applicable, with Recommendation 10: Customer Due Diligence, as outlined in the FATF 40 Recommendations.

The following elements of CDD should be carried out for all customers, no matter the customer type.

4.2.1.1. Customer Identification and Verification

Under Article 8 of the AML-CFT Decision, LFIs are required to identify and verify the identities of all customers. Customers must generally be identified and verified prior to establishing a business relationship. Full detail regarding customer identification and verification can be found in the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 6.3.1.

4.2.1.2. Beneficial Owner Identification and Verification

Under Article 9 of the AML-CFT Decision, LFIs are required to identify and verify the identities of all beneficial owners of any legal person customer. For more details regarding beneficial ownership identification and verification and other CDD measures for legal persons and arrangements, please consult the CBUAE's *AML/CFT Guidelines for Financial Institutions*, sections 6.3.1 and 6.3.3, respectively, as well as the *CBUAE's Guidance for LFIs Providing Services to Legal Persons and Arrangements*.[23]

4.2.1.3. Understanding the Nature of the Customer's Business and the Nature and Purpose of the Business Relationship

Under Article 8 of the AML-CFT Decision, LFIs are required to understand the nature of the customer's business as well as the nature and purpose of the LFI's relationship with the customer, including the expected uses to which the customer will put the LFI's products or services. This step requires the LFI to collect information that allows it to create a profile of the customer, including the types and volumes of transactions the customer is expected to engage in, and to assess the risks associated with the relationship. In certain instances, the expected type and volume of transactions are implicit in the specific product or service being provided, in which case this aspect of the customer's profile can be derived directly from the product choice.

Obtaining a sufficient understanding of its customers and the nature and purpose of the customer relationship—together with the ongoing analysis of actual customer behaviour and the behaviour of relevant peer groups—allows the LFI to develop a baseline of normal or expected activity for the customer, against which unusual or potentially suspicious transactions or activity can be identified. This element of CDD can also serve to inform the LFI's risk rating or other risk assessment of the customer for the purposes of

[23] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

performing risk-based ongoing monitoring (see section 4.2.1.4) and determining whether enhanced due diligence measures may be warranted (see section 4.2.3).

Measures to understand the nature of a customer's business and the nature and purpose of the LFI's relationship to the customer should include:

- **Determining if a customer is a VASP:** In the context of VASPs and VA activities, a key element of understanding the nature of a customer's business is determining whether a customer meets the definition of a VASP (as provided in section 1.5 above), regardless of whether the customer is currently licensed or registered as a VASP or whether it considers itself to be or markets itself as a VASP. As part of this assessment, LFIs should determine whether a customer's NFT-related business activities constitute covered VASP activities. To this end, LFIs should require their customers to provide a certification or attestation indicating whether they engage in each of the covered VASP activities detailed in section 1.5, as VASP customers may not be aware of the full range of transactions and services that constitute VASP activities for AML/CFT purposes. Such a certification or attestation should be obtained at onboarding or, for existing customers, as part of ongoing CDD monitoring (as described in section 4.2.1.4 below) and should be subject to verification by the LFI on a risk basis, including based on the risk of the LFI's sector or upon identification of ML/TF red flag indicators (as presented in Annex B).
    - Where an LFI has identified a customer that it believes may be engaged in covered VASP activities, it should notify the customer and request additional information to inform a conclusive determination of whether the customer is a VASP.
    - If an LFI determines that a customer is a VASP, it should ensure that it is licensed to operate as a VASP by relevant authorities in the UAE and should perform the specific due diligence measures outlined in section 4.2.2 below, in addition to the general CDD measures outlined in this section.
- **For VASP customers, understanding which VASP activities it conducts and the nature of its customers and geographies:** The LFI should gather sufficient information about the VASP to understand fully the nature of its business, including the specific VASP activities it conducts, its customer base, and the geographic markets in which it operates or that it serves or intends to serve.
- **Determining if a customer provides downstream services to third-party VASPs:** Additionally, LFIs should obtain an understanding of whether the customer intends to use its account or relationship with the LFI to provide downstream services to other VASPs.
    - If an LFI determines that VASP customer intends to provide services to third-party VASPs through its account or relationship with the LFI, the LFI should perform the EDD measures outlined in section 4.2.3.1 below, in addition to the general CDD measures outlined in this section and the specific due diligence measures outlined in section 4.2.2.

- **Determining the nature of a customer's intended use of the LFI to facilitate VA activity:** Finally, LFIs should obtain an understanding of whether and to what extent a customer (other than an FI or VASP) intends to use its account or relationship with the LFI to send or receive funds on its own behalf for the purposes of exchanging virtual assets for fiat currency or vice versa. Specifically, LFIs should seek to identify customers that intend to use their account or relationship with the LFI to conduct a high volume or value of virtual asset exchange transactions (such as businesses that accept payment in VA and expect to regularly convert these proceeds into fiat currency) and/or to conduct VA transactions with foreign VASPs located in jurisdictions considered to be high risk for ML/TF. As part of this assessment, LFIs should obtain an understanding of the nature of their customers' proprietary transactions involving NFTs and determine whether such NFTs are used for payment or investment purposes in practice and thus fall under the definition of a VA.
    - If an LFI determines that a customer (other than an FI or VASP) intends to conduct a high volume or value of VA transactions and/or to conduct VA transactions with foreign VASPs located in high-risk jurisdictions, it should consider applying enhanced ongoing monitoring, as outlined in section 4.2.3.2 below, taking into account the totality of the customer's business and risk profile.
    - LFIs should also require customers engaging or expecting to engage in VA activity to attest that they will not use their account or relationship with the LFI to transact with VASPs operating in the UAE that are not licensed to perform VASP activities by UAE authorities.

4.2.1.4. Ongoing Monitoring

Under Article 12 of the AML-CFT Decision, LFIs are required to subject all customers to ongoing monitoring throughout the business relationship to ensure that the CDD information they hold on all customers is accurate, complete, and up to date. Full detail regarding ongoing monitoring of the business relationship can be found in the CBUAE's *AML/CFT Guidelines for Financial Institutions*, section 6.3.5.

Where a customer is identified as a VASP or as conducting VA transactions in high volumes or values and/or with a VASP in a high-risk jurisdiction, the LFI should reassess the customer's risk profile and apply, where applicable, the specific and enhanced due diligence measures detailed in sections 4.2.2 and 3.2.3 below. Where an LFI identifies an existing customer that meets the definition of a VASP but does not currently have a valid license to operate in the UAE (including where the customer's license to operate as a VASP has lapsed or been revoked or suspended) the LFI should stop all transaction activity with or through the LFI until the customer has obtained the license from applicable UAE authorities and provided a copy of the license to the LFI.

4.2.1.5. Sanctions Screening

An LFI should screen the following parties against lists of sanctioned persons, internal watchlists (such as lists of customers previously exited for financial crime reasons), and, on a risk basis, relevant ML/TF information sources (such as negative media databases) prior to a customer's onboarding:

- All customers, regardless of risk rating or risk profile;
- Beneficial owners of legal entity customers;
- Directors, partners, and managers of customers that are legal persons; and
- Natural persons having executive authority over customers that are legal arrangements.

With respect to sanctions lists, the parties listed above should be screened prior to a customer's onboarding and on an ongoing basis thereafter. Please see section 4.4 below.

The results of screening and assessment by the LFI should be documented. For more details and information, please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening.*[24]

4.2.1.6. Customer Rejection and Exit

Prior to establishing a business relationship, if an LFI has any reasonable grounds to suspect that the assets or funds of a customer are the proceeds of crime or related to the financing of terrorism, the LFI should reject the business relationship and, per Article 17 of the AML-CFT Decision, file a suspicious activity report ("SAR") with the UAE Financial Intelligence Unit ("FIU"). Additionally, as per Article 13 of the AML-CFT Decision and Article 15 of Cabinet Decision 74, where an LFI is unable to undertake the CDD measures described above, or is a confirmed match to a party included on applicable sanctions lists, the LFI must not onboard the customer, must exit the relationship if one has been established, and must not transfer any funds to, on behalf of, or for the benefit of the customer.

4.2.2. *Specific Due Diligence for <u>All</u> VASP Customers*

Upon determining that a customer is a VASP as per the definition provided in section 1.5 above, LFIs should undertake the following specific due diligence measures, in addition to the general CDD measures described above:

- **Obtain a copy of the VASP's license to operate in the UAE.** Before establishing a new customer relationship or conducting any business with a VASP—defined as an individual or entity that performs one or more of the VASP activities specified in section 1.5—LFIs should obtain a copy of the VASP's license to operate as a VASP in the UAE or an NOC addressed to the LFI from the applicable UAE licensing authority indicating that the VASP may be provided an account in preparation for being granted a valid license. The VASP's client money servicing operations on such account may only commence once it has received a formal license from the appropriate UAE authority.
    - The LFI should also obtain an understanding of whether the VASP is duly licensed, registered, or otherwise authorized to engage in VASP activities wherever it operates internationally; however, LFIs are expected to obtain copies of licenses issued outside the

[24] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

UAE only on a risk basis. For example, LFIs may request the copies of licenses from VASPs licensed in high-risk jurisdictions orfrom VASPs in other jurisdictions that offer services and/or assets deemed to carry a higher level of risk.

- **Understand and assess the VASP's reputation.** The LFI should gather sufficient information and determine from publicly available information (including via third-party databases and screening tools) the reputation of the VASP, including a determination of whether (and when) it has been subject to an ML/TF investigation or regulatory action, whether in the UAE or from relevant foreign authorities. In the case of a newly formed VASP, such an assessment should focus on the reputation of the VASP's beneficial owners and their relevant prior or ongoing business activities.
    - Where the LFI identifies indicators of heighted ML/TF risk related to the VASP's reputation, it should apply the EDD measures outlined in section 4.2.3.1 below before onboarding or conducting any business with the customer.
- **Assess the VASP's AML/CFT controls.** The LFI should assess the VASP's AML/CFT controls, either through a review of the VASP's written AML/CFT program or framework, or through the use of a suitable questionnaire (modelled, for example, on the Wolfsberg Group's Financial Crimes Compliance Questionnaire). The assessment should include confirming that the VASP's AML/CFT controls are subject to independent audit, whether internal or external, and that the VASP's transaction monitoring, sanctions screening, and other relevant AML/CFT systems are subject to an annual assessment and model validation by a qualified, independent third party.
    - LFIs should be aware that, with limited modifications, the preventive measures set out in Recommendations 9 to 21 of the FATF Standards apply to VASPs in the same manner as they apply to FIs.
    - The LFI's assessment of its VASP customers' AML/CFT controls should include a determination of whether the VASP's AML/CFT program requires the VASP to implement funds transfer recordkeeping and "travel rule"[25] requirements as set forth in Articles 27 and 33 bis 1 of the AML-CFT Decision, as amended, including the obligation to obtain, hold, and submit required originator and beneficiary information associated with VA transfers in order to identify and report suspicious transactions, take freezing actions, and prohibit transactions with designated persons and entities.
    - Where the LFI identifies serious deficiencies or gaps in the VASP's AML/CFT controls, it should apply the EDD measures outlined in section 4.2.3.1 below before onboarding or conducting any business with the customer.
- **Understand and assess the VASP's activity on behalf of third parties.** The LFI should understand how the VASP will be using its relationship with the LFI to hold funds for or provide

[25] The "travel rule" refers to the application of the FATF's wire transfer requirements (per Recommendation 16) in the VA context. Travel rule requirements apply to both VASPs and other obliged entities such as FIs when they send or receive VA transfers on behalf of a customer.

services to the VASP's underlying customers (as opposed to engaging in exclusively proprietary activity on its own behalf, using its own funds) and assess the nature and level of risk associated with such arrangements. As part of this process, the LFI should determine if its VASP customers provide accounts or custodial wallets for downstream customers that are themselves VASPs (also known as "third-party VASPs") and whether such accounts can be used directly by customers of the third-party VASP to transact business on the customer's own behalf. Such arrangements present risks similar to those of "nested" correspondent banking relationships and should be subject to heightened scrutiny and monitoring.

- Where the LFI's VASP customer intends to transact with or through the LFI on behalf of a third-party VASP, the LFI should apply the enhanced due diligence measures outlined in section 4.2.3.1 below.

If, based on its internal risk assessment, an LFI decides to reject or discontinue a customer relationship with a VASP that has been duly licensed by a competent authority in the UAE, the LFI should notify the licensing authority immediately and present the findings of its risk assessment.

Once the above due diligence measures—and any EDD measures, as appropriate—have been completed, **the LFI should obtain approval from senior management before onboarding or conducting business with a VASP.**

4.2.3. *Enhanced Measures for Higher-Risk Customers*

LFIs are expected to implement appropriate policies and procedures to determine whether relationships with or transactions undertaken for or on behalf of a customer present a higher risk for ML or TF. In the context of VASPs and VA activity, examples of potentially higher-risk scenarios include, but are not limited to, those in which:

- The LFI identifies indicators of heighted ML/TF risk related to the VASP's reputation;
- The LFI identifies serious deficiencies or gaps in the VASP's AML/CFT controls;
- The LFI's VASP customer transacts or intends to transact with or through the LFI on behalf of a third-party VASP; and
- The LFI determines that a customer (other than an FI or VASP) uses or intends to use its account or relationship with the LFI to conduct a high volume or value of VA exchange transactions and/or to conduct transactions with VASPs in jurisdictions identified as high risk for ML/TF.

Section 4.2.3.1 below covers EDD measures for *VASP customers* identified as presenting heightened risks, while section 4.2.3.2 covers enhanced ongoing monitoring measures that may be applied—taking into account the totality of the customer's risk profile—to *customers other than VASPs or FIs* that conduct a high volume or value of VA exchange activity.

4.2.3.1. EDD for High-Risk VASP Customers

Where LFIs have identified indicators of heightened risk related to a VASP customer, they should perform a more in-depth review of the VASP's AML/CFT compliance program. Such a review can include, on a risk basis:

- Reviewing the VASP's AML/CFT policies or relevant systems and controls framework, AML/CFT risk assessment, AML/CFT independent audit, and independent model validation results;
- Interviewing the VASP's compliance officer(s); and/or
- Conducting a third-party review or on-site visit of the VASP.

In general, LFIs should implement additional control measures when dealing with high-risk VASP customers, including, as appropriate, restricting VA transfers to within their customer base (i.e., internal transfers of VAs within the same VASP), only allowing confirmed first-party transfers outside of their customer base (i.e., where the originator and beneficiary are confirmed to be the same person), and enhanced monitoring of transactions. There is an expectation that LFIs reject or exit relationships with high-risk VASP customers, when the LFI determines it is unable to fully manage the risks presented by the customer relationship through the application of enhanced controls.

In addition, for VASP customers that transact or intend to transact with or through the LFI on behalf of a third-party VASP, the LFI should:

- Obtain information from the VASP customer regarding the existence of any relationships with third-party VASPs and the locations in which any such VASPs conduct business;
- Ensure specifically that the VASP customer understands and implements international payment transparency and "travel rule" standards, including by obtaining and screening all required originator and beneficiary information and, where necessary, identifying and performing due diligence on non-customer VASP counterparties; and
- Have measures in place to detect potential, undisclosed relationships with third-party VASPs provided by the VASP customer (e.g., transaction monitoring scenarios designed to identify third-party activity typical of a VASP or keyword searches that match a third party's name to an internal list of known VASP entities) and take appropriate follow-up action when the VASP customer does not disclose the existence of such a relationship.

As above, if, based on its internal risk assessment, an LFI decides to reject or discontinue a customer relationship with a VASP that has been duly licensed by a competent authority in the UAE, the LFI should notify the licensing authority immediately and present the findings of its risk assessment.

LFIs should also consider subjecting any VASP customers categorized as high risk to more frequent or more intensive ongoing monitoring, as described in section 4.2.1.4 above.

4.2.3.2. Enhanced Ongoing Monitoring for Customers Conducting Higher-Risk VA Activity

Where LFIs determine that a customer (other than an FI or VASP) uses or intends to use its account or relationship with the LFI to conduct a high volume or value of VA exchange transactions and/or to conduct

transactions with VASPs in jurisdictions identified as high risk for ML/TF, they should perform more frequent, intensive, and focused ongoing monitoring. LFIs should review the CDD files of higher-risk customers on a frequent basis, such as every six or nine months for very high-risk customers. The methods LFIs use to review the account or relationship should also be more intensive and should not rely solely on information supplied by the customer. For example, LFIs should consider:

- Reviewing more or even all transactions on the account during the review period, rather than a sample of transactions;
- Conducting a meeting between the LFI and the customer's managing director, Chief Financial Officer, or other senior leadership if the LFI is not satisfied with the documentation provided by the customer, during which the LFI should request an attestation that any specific transactions under review are not related to illicit activities;
- Conducting searches of public databases, including news and government databases, to independently identify material changes in a customer's ownership or business activities and to identify adverse media reports. Such searches should include adverse media searches of public records and databases, using relevant key words, including but not limited to allegation, fraud, corruption, and laundering; and
- Utilizing geolocation tools and internet protocol ("IP") address blocking controls to detect and prevent access to financial services from IP addresses that originate in high-risk jurisdictions and to identify behavioural patterns that would be difficult to establish otherwise. Analytic tools can identify IP misattribution, for example, by screening IP addresses against known virtual private network ("VPN") IP addresses and identifying improbably logins.

4.3. Transaction Monitoring and Suspicious Transaction Reporting

4.3.1. *Transaction Monitoring*

Under Article 16 of the AML-CFT Decision, LFIs must monitor activity by all customers to identify behaviour that is potentially suspicious and that may need to be the subject of an STR or SAR.

In the context of VASPs and VA-related risks, LFIs should ensure that transaction monitoring rules or keyword searches are designed and updated with sufficient frequency to allow the LFI to detect undisclosed VASP activity as well as significant transactions between their customers (other than FIs and VASPs) and third-party VASPs. Whether using automated systems or manual processes, LFIs should monitor transactions for recognized indicators of suspicious VA activities or possible attempts to evade targeted financial sanctions and AML/CFT reporting requirements or other controls. VA-related red flags identified by supervisors, law enforcement, and other authorities as specific to the UAE include:

- Receipt of funds from recognised or apparent VASP customers—as well as non-VASP, non-FI customers identified as engaging in high volumes or values of VA transactions and/or VA

transactions with foreign VASPs in high-risk jurisdictions—in small multiples potentially below the daily cash reporting threshold to avoid triggering system alerts;

- Relationships and transactions with third-party payment providers and payment gateways, which in turn may deal with VAs and/or VASPs, including through OTC brokers that facilitate trades between individual buyers and sellers who are not willing to transact on an open exchange, and through peer-to-peer ("P2P") platforms;
- One-off transactions;
- Fewer high-value inbound payments and numerous low-value outbound transfers;
- Transactions in multiple foreign currencies;
- Relationships or transactions with legal entity customers operating in the information technology ("IT"), software, or technology sectors or with sub-contracted industry intermediaries; and
- Returned payments.

Annex B contains a list of red flag indicators that LFIs should incorporate, where applicable, into their transaction monitoring rules and processes, as well as transaction-specific reviews.

LFIs should ensure close coordination between their transactions monitoring and sanctions screening teams, on the one hand, and cybersecurity and fraud units, on the other, to triage potentially illicit transactions and other risk events and identify potential cases of virtual asset use to circumvent AML/CFT controls and/or evade targeted financial sanctions. Based on the size, complexity, and overall risk profile of the institutions, LFIs should consider performing VA exposure and risk analyses to maintain an up-to-date understanding of their direct or indirect exposure to VAs and VASPs and to apply enhanced controls on a risk-sensitive basis.

For more details and information, please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening.*[26]

4.3.2. *STR Reporting*

Under Article 15 of the AML-CFT Law and Article 17 of AML-CFT Decision, LFIs are required to file an STR or SAR or other report types with the UAE FIU when they have reasonable grounds to suspect that a transaction, attempted transaction, or certain funds constitute, in whole or in part, regardless of the amount, the proceeds of crime, are related to a crime, or are intended to be used in a crime. Please consult the CBUAE's *Guidance for LFIs on Suspicious Transaction Reporting* for further information.[27] LFIs should also consult any incremental reporting requirements or guidelines set forth by the UAE's VASP regulatory and supervisory authorities, as these may reflect emerging risks, trends, and typologies relevant to the VA sector as a whole.

[26] Available at: https://www.centralbank.ae/en/cbuae-amlcft.
[27] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

4.4. Sanctions Obligations and Freezing Without Delay

The AML-CFT Law and AML-CFT Decision require LFIs to promptly apply directives issued by the competent authorities of the UAE for implementing the decisions issued by the United Nations Security Council ("UNSC") under Chapter VII of the Charter of the United Nations ("UN"). In furtherance of this requirement, the Cabinet Decision No. (74) of 2020 sets out the legislative and regulatory framework regarding the Targeted Financial Sanctions ("TFS"), including the Local Terrorist List and the UN Consolidated List.

As LFIs in the UAE do not accept VAs directly or process the VA side of a VA-to-fiat or fiat-to-VA exchange transaction, LFIs will not have the ability, and therefore will not have the obligation, to freeze VAs directly. Rather, LFIs' obligations to freeze without delay pertain to funds or other assets held by the LFI and subject to appropriate sanctions requirements. To the extent that LFIs do come into possession of VAs subject to freezing measures, they will be subject to the same obligations to freeze those assets without delay and comply with related requirements under Cabinet Decision No. (74).

For more information and details on their obligations in relation to their sanctions obligations, LFIs should consult the Executive Office for Control and Non-Proliferation's ("Executive Office's") "*Guidance on Targeted Financial Sanctions for Financial Institutions and designated non-financial business and professions*";[28] the "CBUAE *Guidance for Licensed Financial Institutions on the Implementation of Targeted Financial Sanctions*" as well as the "*CBUAE Guidance for Licensed Financial institutions on Transaction Monitoring Screening and Sanctions screening*"[29] and any of their amendments or updates thereof.

4.5. Training

As with all risks to which the LFI is exposed, the AML/CFT training program should ensure that employees are aware of the risks related to VAs and VASPs, are familiar with the obligations of the LFI, and are equipped to apply appropriate risk-based controls. Training should be tailored and customized to the LFI's risk and the nature of its operations and should be clearly documented in the LFI's AML/CFT compliance program and associated training policies, procedures, plans, materials, and attendance records.

4.6. Governance and Independent Audit

The specific preventive measures discussed above should take place within, and be supported by, a comprehensive institutional AML/CFT program that is appropriate to the risks the LFI faces and organized in accordance with the "three lines of defence" model. All three lines of defence should report up to and have the active support and oversight of the LFI's senior management, defined broadly to include executives, senior leadership, and the Board of Directors. See section 8 of the *Guidelines on Anti-Money*

[28] Available at: https://www.uaeiec.gov.ae/en-us/un-page.
[29] Available at: https://www.centralbank.ae/en/cbuae-amlcft

Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions for additional detail.[30]

4.7. Record Keeping

According to Article 16 of the AML-CFT Law and Article 24 of the AML-CFT Decision, LFIs must maintain detailed records associated with their ML/FT risk assessment and mitigation measures, as well as records, documents, data, and statistics for all financial transactions, records obtained through CDD measures and ongoing monitoring (including copies of personal identification documents), account files and business correspondence, and STRs/SARs and results of any analysis performed. LFIs should maintain the records in an organized manner so as to permit data analysis and the tracking of financial transactions. Records should be sufficient to permit reconstruction of individual transactions so as to provide, if necessary, evidence for prosecution of criminal activity. LFIs should make the records available to the competent authorities immediately upon request. Consistent with local regulatory requirements, all LFIs must ensure compliance with Recommendation 11: Record Keeping, as outlined in the FATF 40 Recommendations.

The aforementioned provisions also require that all records be retained for at least five (5) years from the date of completion of the transaction or termination of the business relationship with the customer, or from the date of completion of the inspection by the CBUAE, or from the date of issuance of a final judgment of the competent judicial authorities, or liquidation, dissolution, or other form of termination of a legal person or arrangement, all depending on the circumstances.

5. Mitigating ML/TF Risks Related to LFIs' Proprietary Investments in VAs

LFIs should understand, assess, and take appropriate steps to mitigate the ML/TF risks related to their own proprietary investments in virtual assets: that is, investments in VAs made by LFIs on their own behalf, for their own benefit, and using their own funds. Measures to understand and mitigate ML/TF risk should be undertaken *in addition to* any measures required to satisfy the evolving prudential standards that have been set forth by international bodies such as the Basel Committee on Banking Supervision, which include proposed credit and market risk requirements based on the type of VA or other digital asset to which a given bank may be exposed.

With respect to ML/TF risk, LFIs should ensure that any proprietary investment in VAs is made through a VASP that is duly licensed or registered by relevant local authorities in a jurisdiction that has adequate AML/CFT regulation and supervision with respect to virtual assets. If the VASP operates in the UAE, it should be licensed by UAE authorities, as discussed in section 2.4 above. If the VASP is not licensed to operate in the UAE, it should be licensed or registered, at a minimum, in the jurisdiction(s) in which it was

[30] Available at: https://www.centralbank.ae/en/cbuae-amlcft.

created, is headquartered, or maintains a primary operating presence (where the VASP is a legal person) or the jurisdiction in which its place of business is located (where the VASP is a natural person).

The following sections explain the specific and, as warranted, enhanced due diligence measures that LFIs should perform on any VASP with which it seeks to conduct proprietary VA transactions (hereafter, a "VASP counterparty"). LFIs should review due diligence information on VASP counterparties periodically on the basis of risk (i.e., with higher-risk VASP counterparties subject to more frequent periodic reviews) and upon the occurrence of specified "trigger events," such as a material change in the VASP's risk profile.

Finally, note that an LFI's use of a proprietary account or virtual asset wallet to conduct virtual asset exchange or transfer activities *on its own behalf, for its own benefit, and using its own funds* does not constitute a VASP activity, as defined in section 1.5 above, which stipulates that a person engaged in one or more of the specified activities qualifies as a VASP only if it does so *as a business* and *for or on behalf of another natural or legal person*. Likewise, an LFI's administration of safekeeping of its own, proprietary virtual assets in a virtual asset wallet does not constitute a VASP activity or otherwise subject the LFI to requirements and expectations for licensed VASPs, provided that it does not as a business conduct such administration or safekeeping services for or on behalf of another natural or legal person.

5.1.1. *Specific Due Diligence for All VASP Counterparties*

Before conducting a proprietary VA transaction with a VASP counterparty, LFIs should undertake the following specific due diligence measures:

- **Obtain a copy of the VASP counterparty's license to operate or evidence of registration, as applicable.** For local VASPs, LFIs should obtain a copy of the VASP's license to operate as a VASP in the UAE. For foreign VASPs that are not also licensed to operate by UAE authorities, LFIs should obtain a copy of its license to operate or evidence of its registration with local authorities.
- **Understand and assess the VASP counterparty's reputation and, for any foreign VASP counterparty, the quality of its AML/CFT supervision.** The LFI should gather sufficient information and determine from publicly available information the reputation of the VASP, including a determination of whether (and when) it has been subject to an ML/TF investigation or regulatory action, whether in the UAE or, regarding any operating locations outside of the UAE, from relevant foreign authorities. For VASPs licensed or registered outside of the UAE, LFIs should determine whether the VASP is subject to an effective AML/CFT regulatory and supervisory regime, including especially the extent to which the regime requires VASPs to implement AML/CFT preventive measures and effectively monitors them for compliance. The LFI's assessment of the VASP's reputation should include a determination of whether (and when) it has been subject to an ML/TF investigation or regulatory action. In the case of a newly formed VASP, such an assessment should focus on the reputation of the VASP's beneficial owners and their relevant prior or ongoing business activities.

- Where the LFI identifies indicators of heighted ML/TF risk related to the VASP's reputation or supervisory regime, it should apply the EDD measures outlined in section 5.1.2 below before conducting any proprietary VA transactions with the VASP counterparty.

- **Assess the VASP counterparty's AML/CFT controls.** The LFI should assess the VASP's AML/CFT controls, either through a review of the VASP's written AML/CFT program or framework, or through the use of a suitable questionnaire (modelled, for example, on the Wolfsberg Group's Financial Crimes Compliance Questionnaire). The assessment should include confirming that the VASP's AML/CFT controls are subject to independent audit, whether internal or external, and that the VASP's transaction monitoring, sanctions screening, and other relevant AML/CFT systems are subject to an annual assessment and model validation by a qualified, independent third party.
    - As noted above, LFIs should be aware that, with limited modifications, the preventive measures set out in Recommendations 9 to 21 of the FATF Standards apply to VASPs in the same manner as they apply to FIs.
    - Where the LFI identifies serious deficiencies or gaps in the VASP's AML/CFT controls, it should apply the EDD measures outlined in section 5.1.2 below before conducting any proprietary VA transactions with the VASP counterparty.

5.1.2. *Enhanced Measures for High-Risk VASP Counterparties*

LFIs are expected to implement appropriate policies and procedures to determine whether relationships or transactions with a VASP counterparty present a higher risk for ML or TF. In the context of LFIs' proprietary investments in VAs with or through a VASP counterparty, examples of potentially higher-risk scenarios include, but are not limited to, those in which:

- The LFI identifies indicators of heighted ML/TF risk related to the VASP's reputation; or
- The LFI identifies serious deficiencies or gaps in the VASP's AML/CFT controls.

Where LFIs have identified indicators of heightened risk related to a VASP counterparty, they should perform a more in-depth review of the VASP's AML/CFT compliance program. Such a review should include, on a risk basis:

- Reviewing the VASP's AML/CFT policies or relevant systems and controls framework, AML/CFT risk assessment, AML/CFT independent audit, and independent model validation results;
- Interviewing the VASP's compliance officer(s); and/or
- Conducting a third-party review or on-site visit of the VASP.

In general, VASPs should implement additional control measures when dealing with high-risk VASP customers or VA transactions in countries with weak AML/CFT implementation, including, as appropriate, restricting VA transfers to within their customer base (i.e., internal transfers of VAs within the same VASP), only allowing confirmed first-party transfers outside of their customer base (i.e., where the originator and

beneficiary are confirmed to be the same person), periodic name screening, and enhanced monitoring and screening of transactions.

LFIs should also consider subjecting any VASP customers categorized as high risk to more frequent or more intensive ongoing monitoring, as described above.

Annex A: Vulnerabilities Associated with Other VASP Business Models

In addition to understanding the risks associated with VASPs already licensed and operational in the UAE, LFIs should also be aware of the vulnerabilities associated with other VASP business models and product features, as the VASP operating environment is rapidly evolving and subject to new entrants and changes in existing business models. In addition to the business models discussed in section 2.2 above, LFIs should note the vulnerabilities associated with the following types of virtual asset services and activities. Note that the descriptions and examples presented below are provided for illustrative purposes only and are not intended to be comprehensive.

- **Payment Processors:** Payment processors provide a variety of services that enable merchants to accept virtual assets as payment for goods and services. Certain processors may also be classified as virtual asset exchanges, depending on the nature of the services they provide. Payment processor services may include:
    - Allowing users to send fiat currencies to their accounts at virtual asset exchanges, particularly when the exchange is not able to obtain banking services itself;
    - Accepting virtual assets from the merchant's customers and converting them to fiat currencies on behalf of the merchant; and
    - Offering a user-friendly interface that enables a merchant's customers to carry out decentralized P2P transactions using basic blockchain technology.[31]

  Payment processors may be involved directly in financial crime and are also exposed to illicit finance risk based on their clients' activities. Authorities internationally have taken action against payment processors and their owners on charges of money laundering and involvement in drug trafficking. In one case, a payment processor was found to have lied to banks regarding the purpose of accounts it was seeking to open, telling the financial institutions that the accounts would be used for real estate investments when in fact the accounts were used to service virtual asset exchanges that lacked direct access to banks. This processor may also have been involved in a much larger fraud involving its main client, a large virtual asset exchange.
- **Virtual Asset Wallets:** Virtual asset wallets are software programs that store virtual assets while making them easily available for transactions. Hosted wallets are maintained on servers belonging

[31] Whether a self-described "P2P" platform constitutes a VASP depends on the nature of the services provided, not on its self-description of the type of technology employed. P2P entities that provide very limited functionality falling short of exchange, transfer, safekeeping, administration, control, and the provision of financial services associated with issuance will generally not be considered VASPs. These may include, for example, websites that offer only a forum for buyers and sellers to identify and communicate with each other without offering, even in part, those services that constitute VASP activities, as defined in section 1.5 above. However, most "matching" or "finding" services currently in operation—even if they self-categorize as "P2P" platforms—may have at least some party involved at some stage of the product's development and launch that constitutes a VASP. Automating a process that has been designed to provide covered services for a business does not relieve the controlling party of VASP obligations.

to a company that provides virtual wallet services. The host will generally also be responsible for processing transactions and for providing security; a hosted wallet is somewhat analogous to a traditional checking account. Unhosted wallets are directly maintained by the owner of the virtual assets without the involvement of a third party. Unhosted wallets are somewhat analogous to storing cash in a safe at a private home or office—with the added advantage that these assets are always available for transactions no matter where the owner is.

- **Initial Coin Offerings:** ICOs are sales of new virtual assets, or financial interests in such assets, to a group of investors or the general public. Investors in ICOs often must use existing virtual assets to make the investment. Such sales may take place to realize a profit following development of a new virtual asset or blockchain, or to finance the development of a new type of blockchain to produce the new virtual asset. Investors in new ventures related to virtual assets may also receive virtual tokens as proof of investment.
- **Virtual Asset Kiosks:** Kiosks are electronic terminals, also known as a “Crypto ATMs” or “Bitcoin ATMs,” that allow users to trade fiat currencies for convertible virtual currencies and vice versa. Based on the FATF Standards, VA kiosks should be subject to AML/CFT and know-your-customer requirements, meaning that users should generally be required to submit a form of personally identifiable information such as a phone number or driver’s license before creating an account that can be used at a VA Kiosk, in the same way that customers using ATMs for cash withdrawals would need to undergo know-your-customer and customer due diligence processes at a financial institution.
- **Mining Pools:** Pools are groups of persons that combine their computer processing power to increase their chances of being awarded VAs for verifying a block of transactions. Mining pool operators typically distribute VA awards to their members proportional to their donated processing power, which cause them to qualify as VASPs.

Annex B: ML/TF Red Flag Indicators for Virtual Assets

The following red flags represent a sampling of indicators of heightened ML/TF risks related to virtual assets issued by the FATF.[32] Because no single red flag indicator is determinative of illicit or suspicious activity, LFIs should consider the relevant facts and circumstances of each transaction, in keeping with their risk-based approach to compliance.

Note that, as LFIs in the UAE do not accept VAs directly, not all of these indicators will be directly visible to the LFI through manual or automated monitoring of a customer's account. However, AML/CFT compliance personnel should be aware of higher-risk transaction patterns and other risk indicators, which may prompt enhanced transactional or customer due diligence, including through requests for additional information from VASP customers, even if full transactional information is not immediately available to the LFI.

For more details and information, please consult the CBUAE's *Guidance for Licensed Financial Institutions on Transaction Monitoring and Sanctions Screening*[33] and the *Guidelines for Financial Institutions adopting Enabling Technologies*.[34]

Red Flag Indicators Related to Transactions

- Structuring VA transactions (e.g. exchange or transfer) in small amounts, or in amounts under record-keeping or reporting thresholds, similar to structuring cash transactions.
- Making multiple high-value transactions –
    - in short succession, such as within a 24-hour period;
    - in a staggered and regular pattern, with no further transactions recorded during a long period afterwards, which is particularly common in ransomware-related cases; or
    - to a newly created or to a previously inactive account.
- Transferring VAs immediately to multiple VASPs, especially to VASPs registered or operated in another jurisdiction where –
    - there is no relation to where the customer lives or conducts business; or
    - there is non-existent or weak AML/CFT regulation.
- Depositing VAs at an exchange and then often immediately –
    - withdrawing the VAs without additional exchange activity to other VAs, which is an unnecessary step and incurs transaction fees;
    - converting the VAs to multiple types of VAs, again incurring additional transaction fees, but without logical business explanation (e.g. portfolio diversification); or
    - withdrawing the VAs from a VASP immediately to a private wallet. This effectively turns the exchange/VASP into an ML mixer.
- Accepting funds suspected as stolen or fraudulent, such as by –

[32] FATF, *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets*, September 2020, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Virtual-Assets-Red-Flag-Indicators.html.
[33] Available at: https://www.centralbank.ae/en/cbuae-amlcft.
[34] Available at: https://www.sca.gov.ae/assets/747a7cdf/guidelines-for-financial-institutions-adopting-enabling-technologies-2021.aspx.

- depositing funds from VA addresses that have been identified as holding stolen funds, or VA addresses linked to the holders of stolen funds.

Red Flag Indicators Related to Transaction Patterns

Transactions Concerning New Users

- Conducting a large initial deposit to open a new relationship with a VASP, while the amount funded is inconsistent with the customer profile.
- Conducting a large initial deposit to open a new relationship with a VASP and funding the entire deposit the first day it is opened, and that the customer starts to trade the total amount or a large portion of the amount on that same day or the day after, or if the customer withdraws the whole amount the day after. As most VAs have a transactional limit for deposits, laundering in large amounts could also be done through over-the-counter trading.
- A new user attempts to trade the entire balance of VAs, or withdraws the VAs and attempts to send the entire balance off the platform.

Transactions Concerning All Users

- Transactions involving the use of multiple VAs, or multiple accounts, with no logical business explanation.
- Making frequent transfers in a certain period of time (e.g. a day, a week, a month, etc.) to the same VA account –
  - by more than one person;
  - from the same IP address by one or more persons; or
  - concerning large amounts.
- Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency. Such transactions by a number of related accumulating accounts may initially use VAs instead of fiat currency.
- Conducting VA-fiat currency exchange at a potential loss (e.g. when the value of VA is fluctuating, or regardless of abnormally high commission fees as compared to industry standards, and especially when the transactions have no logical business explanation).
- Converting a large amount of fiat currency into VAs, or a large amount of one type of VA into other types of VAs, with no logical business explanation.

Red Flag Indicators Related to Anonymity

- Transactions by a customer involving more than one type of VA, despite additional transaction fees, and especially those VAs that provide higher anonymity, such as anonymity-enhanced cryptocurrency (AEC) or privacy coins.
- Moving a VA that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin.

- Customers that operate as an unregistered/unlicensed VASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of VA transfers on its customer's behalf, and charge higher fees to its customer than transmission services offered by other exchanges. Use of bank accounts to facilitate these P2P transactions.
- Abnormal transactional activity (level and volume) of VAs cashed out at exchanges from P2P platform-associated wallets with no logical business explanation.
- VAs transferred to or from wallets that show previous patterns of activity associated with the use of VASPs that operate mixing or tumbling services or P2P platforms.
- Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces.
- Funds deposited or withdrawn from a VA address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports.
- The use of decentralised/unhosted, hardware or paper wallets to transport VAs across borders.
- Users entering the VASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS) that suppress or redact the owners of the domain names.
- Users entering the VASP platform using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs. Transactions between partners using various anonymous encrypted communication means (e.g. forums, chats, mobile applications, online games, etc.) instead of a VASP.
- A large number of seemingly unrelated VA wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other.
- Use of VAs whose design is not adequately documented, or that are linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes.
- Receiving funds from or sending funds to VASPs whose CDD or know-your- customer (KYC) processes are demonstrably weak or non-existent.
- Using VA ATMs/kiosks –
    - despite the higher transaction fees and including those commonly used by mules or scam victims; or
    - in high-risk locations where increased criminal activities occur.
- A single use of an ATM/kiosk is not enough in and of itself to constitute a red flag, but would if it was coupled with the machine being in a high-risk area, or was used for repeated small transactions (or other additional factors).

Red Flag Indicators about Senders or Recipients

Irregularities Observed During Account Creations

- Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by VASPs.

- Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious.
- Trying to open an account frequently within the same VASP from the same IP address.
- Regarding merchants/corporate users, their Internet domain registrations are in a different jurisdiction than their jurisdiction of establishment or in a jurisdiction with a weak process for domain registration.

Irregularities Observed During the CDD Process

- Incomplete or insufficient KYC information, or a customer declines requests for KYC documents or inquiries regarding source of funds.
- Sender / recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty.
- Customer has provided forged documents or has edited photographs and/or identification documents as part of the on-boarding process.

Customer Risk Profile Indicators

- A customer provides identification or account credentials (e.g. a non-standard IP address, or flash cookies) shared by another account.
- Discrepancies arise between IP addresses associated with the customer's profile and the IP addresses from which transactions are being initiated.
- A customer's VA address appears on public forums associated with illegal activity.
- A customer is known via publicly available information to law enforcement due to previous criminal association.

Profile of Potential Money Mule or Scam Victims

- Sender does not appear to be familiar with VA technology or online custodial wallet solutions. Such persons could be money mules recruited by professional money launderers, or scam victims turned mules who are deceived into transferring illicit proceeds without knowledge of their origins.
- A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a VA money mule or a victim of elder financial exploitation.
- A customer being a financially vulnerable person, who is often used by drug dealers to assist them in their trafficking business.
- Customer purchases large amounts of VA not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a scam victim.

Other Unusual Behaviour

- A customer frequently changes his or her identification information, including email addresses, IP addresses, or financial information, which may also indicate account takeover against a customer.

- A customer tries to enter into one or more VASPs from different IP addresses frequently over the course of a day.
- Use of language in VA message fields indicative of the transactions being conducted in support of illicit activity or in the purchase of illicit goods, such as drugs or stolen credit card information.
- A customer repeatedly conducts transactions with a subset of individuals at significant profit or loss. This could indicate potential account takeover and attempted extraction of victim balances via trade, or ML scheme to obfuscate funds flow with a VASP infrastructure.

Red Flag Indicators in the Source of Funds or Wealth

- Transacting with VA addresses or bank cards that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites.
- VA transactions originating from or destined to online gambling services.
- The use of one or multiple credit and/or debit cards that are linked to a VA wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing VAs are sourced from cash deposits into credit cards.
- Deposits into an account or a VA address are significantly higher than ordinary with an unknown source of funds, followed by conversion to fiat currency, which may indicate theft of funds.
- Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies or those funds placed in an Initial Coin Offering (ICO) where personal data of investors may not be available or incoming transactions from online payments system through credit/pre-paid cards followed by instant withdrawal.
- A customer's funds which are sourced directly from third-party mixing services or wallet tumblers.
- Bulk of a customer's source of wealth is derived from investments in VAs, ICOs, or fraudulent ICOs, etc.
- A customer's source of wealth is disproportionately drawn from VAs originating from other VASPs that lack AML/CFT controls.

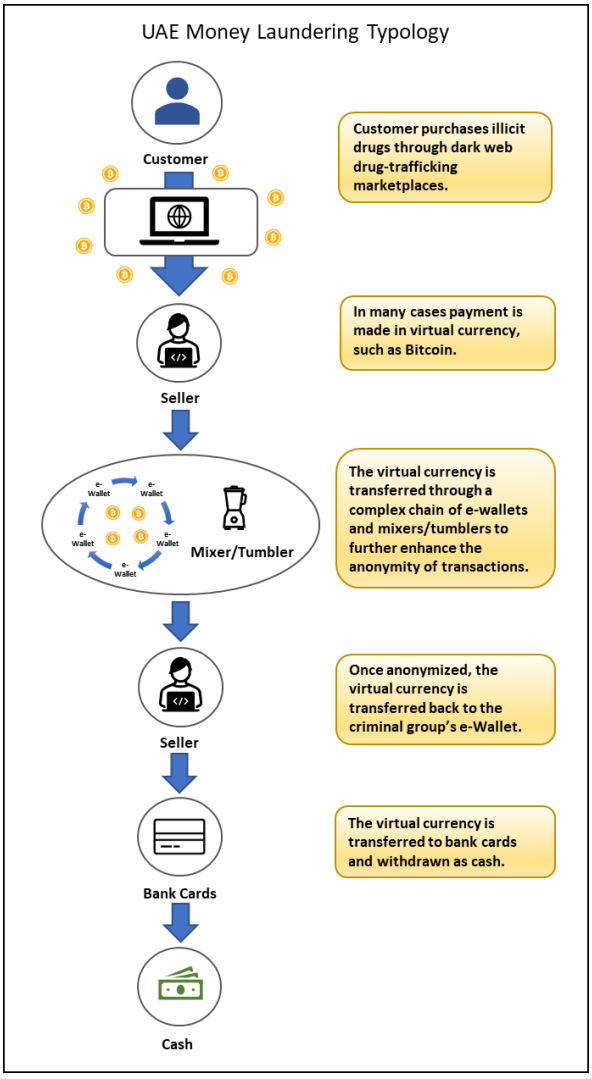
Red Flag Indicators Related to Geographical Risks

- Customer's funds originate from, or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located.
- Customer utilises a VA exchange or foreign-located MVTS in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for VA entities, including inadequate CDD or KYC measures.
- Customer sends funds to VASPs operating in jurisdictions that have no VA regulation, or have not implemented AML/CFT controls.
- Customer sets up offices in or moves offices to jurisdictions that have no regulation or have not implemented regulations governing VAs, or sets up new offices in jurisdictions where there is no clear business rationale to do so.

Annexure C: Infographic on typologies observed in UAE

In many cases, payments for illicit drugs purchased online are transferred to e-wallets held in fiat currency or in virtual currency (e.g., Bitcoin). Afterwards, the virtual currency is transferred through a complex chain of e-wallets, which may include the use of mixers and tumblers to further enhance the anonymity of the virtual currency transactions. Funds are then sent back to the e-wallet of the organized criminal group, and subsequently transferred to bank cards and withdrawn in cash. See the infographic below for an illustration of this typology.

Infographic: Typology of Money Laundering Using Cryptocurrency in the UAE



Other money laundering schemes involving virtual assets that have been identified by authorities in the UAE include schemes relating to drugs, corruption and embezzlement of public funds, and cybercrimes such as ransomware attacks. The use of VAs for illicit purposes may be intensifying in the wake of the COVID-19 pandemic, with scammers offering products that claim to prevent COVID-19 (but that do not in fact exist) in exchange for cryptocurrencies.