Guidance – Regulation of Virtual Asset Activities in ADGM

(VER07.100625)

TABLE OF CONTENTS

INTRODUCTION

1) This Guidance is issued under section 15(2) of the Financial Services and Markets Regulations 2015 ("FSMR") in respect of the Virtual Asset ("VA") regime in ADGM. It should be read in conjunction with FSMR, the relevant Rulebooks of the Financial Services Regulatory Authority ("FSRA"), the FSRA's Guidance & Policies Manual, its *'Guidance – Regulation of Digital Security Offerings and Virtual Assets under the FSMR'* ("ICO Guidance")[1] and its '*Guidance – Regulation of Digital Securities Activities in ADGM'* ("Digital Securities Guidance").[2]

2) This Guidance is primarily applicable to the following Persons:

   a) an Applicant for a Financial Services Permission ("FSP") to carry on a VA Regulated Activity[3] in or from ADGM;

   b) an Authorised Person conducting a VA Regulated Activity; or

   c) a Recognised Investment Exchange with a stipulation on its Recognition Order permitting it to carry on the Regulated Activity of Operating a Multilateral Trading Facility (in relation to Virtual Assets) within ADGM.

3) Certain aspects of this Guidance (e.g., the sections relating to Anti-Money Laundering and Countering Financing of Terrorism and data protection obligations) are also relevant to an Authorised Person conducting a Regulated Activity other than a VA Regulated Activity.

4) This Guidance sets out the FSRA's approach to the regulation of the use of Virtual Assets in ADGM, including activities conducted by Multilateral Trading Facilities, Authorised Persons that are Providing Custody ("Virtual Asset Custodians") and intermediary-type Authorised Persons. This Guidance, together with the applicable ADGM Regulations and FSRA Rules governing the use of Virtual Assets, is collectively referred to as the "Virtual Asset Framework".

5) This Guidance is not an exhaustive source of the FSRA's policy on the exercise of its regulatory functions and powers. The FSRA is not bound by the requirements set out in this Guidance and may:

   a) impose additional requirements to address any specific risks posed in relation to the use of Virtual Assets; and

   b) waive or modify any of the Rules relevant to the Virtual Asset Framework, at its discretion, where appropriate.

[1] https://en.adgm.thomsonreuters.com/rulebook/guidance-regulation-digital-security-offerings-and-virtual-assets-under-financial-services

[2] https://en.adgm.thomsonreuters.com/rulebook/guidance-regulation-digital-securities-activities-adgm

[3] See paragraph 17 for the definition of 'VA Regulated Activity'.

6) Unless otherwise defined or the context otherwise requires, the terms contained in this Guidance have the same meaning as defined in FSMR and the FSRA Glossary Rulebook ("GLO").

7) The term Authorised Person is generally used in this Guidance to refer to an Authorised Person permitted to carry on a VA Regulated Activity or a Recognised Investment Exchange holding a stipulation on its Recognition Order permitting it to operate a Multilateral Trading Facility (in relation to Virtual Assets) (as set out in paragraph 140).[4] Where the context so requires (e.g., in relation to AML obligations), the term Authorised Person should be read as including an Authorised Person conducting Regulated Activities other than VA Regulated Activities.

8) For more details on the process for authorisation as a Multilateral Trading Facility, please contact the FSRA at MIP@adgm.com. For more details on the process for authorisation for any other Virtual Asset business activities, please contact the FSRA at authorisation@adgm.com.

BACKGROUND

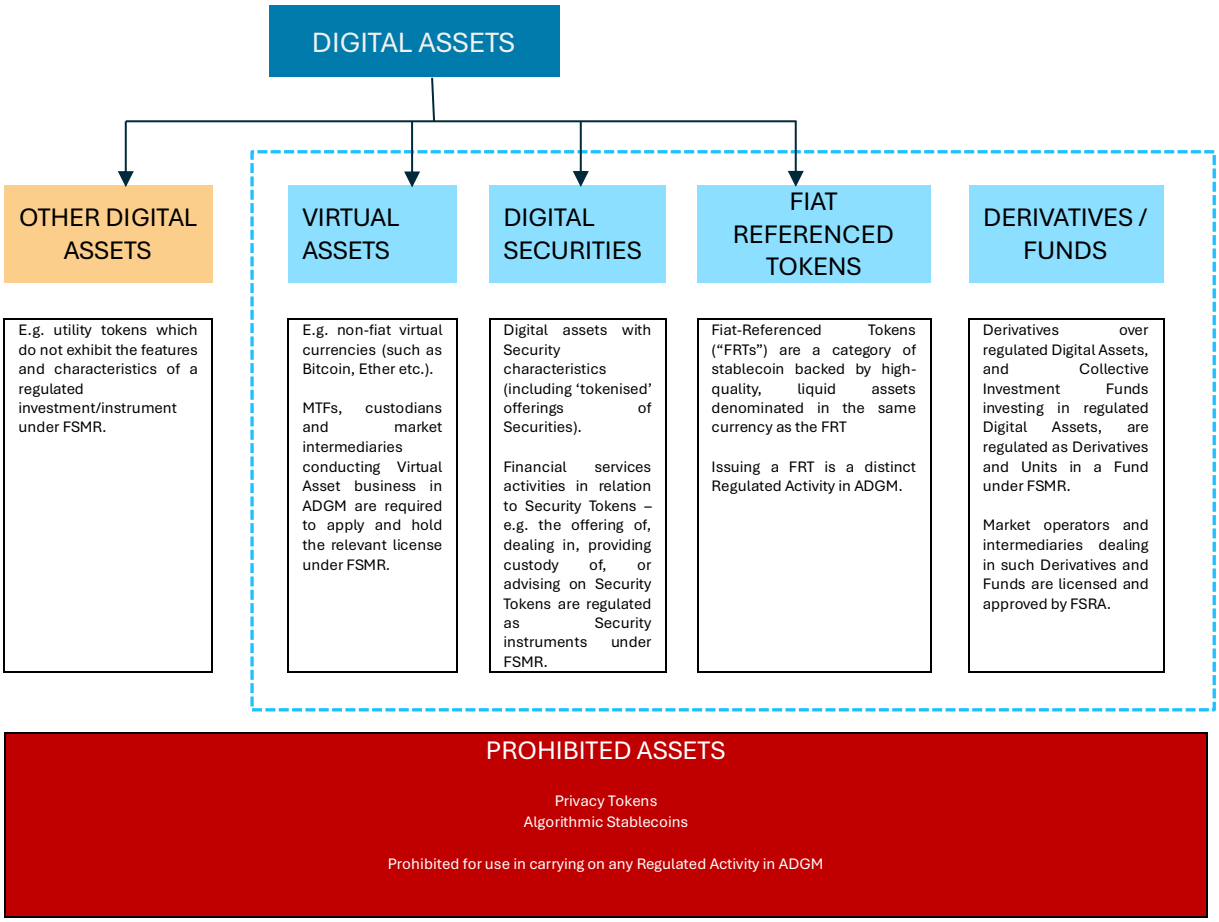
9) Technological innovation is transforming the financial services industry. Constant advances in new technologies have provided opportunities for significant change and disruption to financial services and other related activities globally. Developments in distributed ledger technologies ("DLT") have led to the emergence of various types of digital assets, including virtual coins or tokens for capital raising, and Virtual Assets for the facilitation of economic transactions or the transfer of value.

10) This Guidance primarily focuses on the FSRA's regulatory treatment of Virtual Assets, and the financial services activities that can be conducted in relation to Virtual Assets within ADGM. For the purposes of the Virtual Asset Framework, the FSRA has defined Virtual Assets in FSMR as follows:

> *"**Virtual Asset**" means a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction. A Virtual Asset is -*
>
> *a) neither issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the Virtual Asset;*
>
> *b) distinguished from Fiat Currency and E-money; and*
>
> *c) not a Specified Investment, Fiat-Referenced Token or Spot Commodity."*

11) The diagram and table on the following pages set out the FSRA's regulatory approach in relation to different types of digital assets.

[4] Including in the context of a Recognised Body who has a stipulation for other Regulated Activities set out in its Recognition Order.



The FSRA regulates, and will allow to operate within ADGM, the Digital Assets located within the blue dotted line and Derivatives over/Funds investing in Digital Assets.

Category of Digital Assets / Instruments	Regulatory Approach
"Digital Securities" (e.g., digital/virtual tokens that have the features and characteristics of a Security under FSMR (such as Shares, Debentures and Units in a Collective Investment Fund)).	Deemed to be Securities pursuant to section 58(2)(b) of FSMR. All financial services activities in relation to Digital Securities, such as operating primary / secondary markets, dealing / trading / managing investments in or advising on Digital Securities, are subject to the relevant regulatory requirements under FSMR. Market intermediaries and market operators dealing or managing investments in Digital Securities need to be licensed / approved by FSRA as FSP holders (including as Multilateral Trading Facilities), Recognised Investment Exchanges or Recognised Clearing Houses, as applicable.
"Virtual Assets"	Treated as commodities and, therefore, not deemed Specified Investments under FSMR.

(e.g., non-fiat virtual currencies, crypto 'exchange tokens'). *As stated in paragraph 10, this Guidance is primarily focused on Virtual Assets.*	An Applicant or Authorised Person seeking to conduct a VA Regulated Activity is required to obtain FSRA approval for its proposed Regulated Activities and may only use Approved Virtual Assets in conducting those Regulated Activities. Capital formation activities are not provided for under the Virtual Asset Framework, and such activities are not envisaged under the Market Rulebook (MKT).
Derivatives and Collective Investment Funds of Virtual Assets, Digital Securities and Utility Tokens	Regulated as Specified Investments under FSMR. Market intermediaries and market operators dealing in such Derivatives and Collective Investment Funds will need to be licensed / approved by FSRA as FSP holders, Recognised Investment Exchanges or Recognised Clearing Houses, as applicable.
"Utility Tokens" (e.g., tokens which can be redeemed for access to a specific product or service, typically provided using a DLT platform, do not exhibit the features and characteristics of a regulated investment / instrument under FSMR).	Treated as commodities and, therefore, not deemed Specified Investments under FSMR. Unless such Utility Tokens are caught as Accepted Virtual Assets, spot trading and transactions in Utility Tokens do not constitute Regulated Activities, activities envisaged under a Recognition Order (e.g., those of a Recognised Investment Exchange or Recognised Clearing House), or activities envisaged under MKT.
"Fiat Referenced Tokens (FRTs)" (i.e., stablecoins backed by a single fiat currency that satisfy the definition of FRT)	A FRT is a digital asset, the transfer and storage of which is achieved through the use of distributed ledger or similar technology, the purpose of which is to be used as a medium of exchange with a stable store of value, by: (a) referencing a fixed amount of a single fiat currency; and (b) enabling the holder to redeem the token in exchange for the amount of the fiat currency referred to in (a) from its issuer upon demand. Issuing a FRT is a distinct Regulated Activity in ADGM. An Authorised Person carrying on a Regulated Activity involving a FRT must only use Accepted FRTs (i.e., those approved by the FSRA). FRTs used for VA Regulated Activities must only be Accepted FRTs. FRTs can also be used for denomination, settlement and collateral obligations, amongst other uses, within ADGM. See the section 'Stablecoins' below for guidance on the use of 'stablecoins' that do not satisfy the definition of FRT.

"Privacy Tokens" (e.g., a token which, by design, disguises or otherwise obfuscates, or purports to hide or obfuscate, details of its tokenholder or transaction history which would otherwise be visible to third parties through the DLT on which the token is hosted, and such features cannot be disabled)	Prohibited for use in carrying on any Regulated Activity in ADGM.
"Algorithmic Stablecoins" (e.g., a token which uses, or purports to use, an algorithm as the only or principal means to increase or decrease the supply of tokens in order to stabilise its price or maintain a fixed reference value (peg)).	Prohibited for use in carrying on any Regulated Activity in ADGM.

12) For clarification, the Virtual Asset Framework does not apply to:

a) initial token or coin offerings (ICOs), (whether Digital Securities or Utility tokens), or other capital formation/ capital raising purposes. For details on FSRA's regulatory treatment of ICOs, Digital Securities and utility tokens please refer to the FSRA's ICO Guidance and Digital Securities Guidance;

b) the carrying on of a Regulated Activity involving Fiat-Referenced Tokens;[5]

c) any of the following:

i. the creation or administration of Virtual Assets that are not Accepted Virtual Assets;

ii. the development, dissemination or use of software for the purpose of creating or mining a Virtual Asset;

[5] Certain requirements applicable to the carrying on of VA Regulated Activities also apply to the carrying on of Regulated Activities involving Fiat-Referenced Tokens (e.g., certain Rules in COBS Chapter 17). However, such requirements apply only where Fiat-Referenced Tokens are specifically referenced in the relevant Rule.

iii. a loyalty points scheme denominated in Virtual Assets; or

iv. any other activity or arrangement in relation to Virtual Assets that is deemed by the FSRA to not form part of a Regulated Activity, where necessary and appropriate in order for the FSRA to pursue its objectives.

OBJECTIVES OF THE VIRTUAL ASSET FRAMEWORK

13) Fiat currencies are created and issued by sovereign governments and stored and transferred by banks and other regulated financial institutions on behalf of users. In contrast, the virtual asset ecosystem can enable users to create, store and transfer Virtual Assets without the need for any third party. This creates a set of unique challenges for regulators worldwide. Without regulated entities controlling the creation and use of Virtual Assets, the system is open to significant Financial Crime and other risks.

14) The Virtual Asset Framework is comprehensive in order to effectively address the key risks that the trading of Virtual Assets poses. The FSRA's view is that regulation of AML/CFT risks alone will not sufficiently mitigate certain wider Virtual Asset related risks. Given the increased use of Virtual Assets as a medium for financial transactions, and their connectivity to the mainstream financial system through Virtual Asset and Derivative exchanges and intermediaries, there is the increased potential of contagion risks impacting the stability of the financial sector. There is also no current safety net that ensures that users will be able to recover their Virtual Assets in case of loss or theft.

15) Accordingly, the FSRA has addressed issues around consumer protection, safe custody, technology governance, disclosure/transparency, Market Abuse and the regulation of Multilateral Trading Facilities using Virtual Assets in a manner similar to the regulatory approach taken in relation to securities/derivatives exchanges globally.

FEATURES OF THE VIRTUAL ASSET FRAMEWORK

VA Regulated Activities

16) In accordance with section 30 of FSMR, Applicants that qualify for authorisation to carry on a Regulated Activity will be granted an FSP to carry on the relevant Regulated Activity. An Authorised Person may, as applicable, be required to also obtain FSRA approval in respect of the use of (certain) Specified Investments, Financial Instruments and Virtual Assets as part of its Regulated Activities.

17) While the FSRA continues to monitor developing business models in the Virtual Assets area, at present, an Authorised Person is required to obtain FSRA approval to use Virtual Assets in respect of the following Regulated Activities:

a) Dealing in Investments as Principal;

b) Dealing in Investments as Agent;

c) Advising on Investments or Credit;

d) Arranging Deals in Investments;

e) Managing Assets;

f) Providing Custody; and

g) Operating a Multilateral Trading Facility

(individually, a "VA Regulated Activity" and together the "VA Regulated Activities").

18) To be authorised to conduct a VA Regulated Activity, an Applicant must satisfy the FSRA that all applicable requirements of FSMR and the relevant FSRA Rulebooks have been, and will continue to be, complied with. Upon being granted an FSP, the Applicant will be an Authorised Person for the purposes of FSMR and the FSRA Rulebooks and will have the same regulatory status within ADGM as any other Authorised Person.

19) The principal Rules for Authorised Persons conducting a VA Regulated Activity are set out in Chapter 17 of the Conduct of Business Rulebook ("COBS"). These product specific Rules apply in addition to any other Rules applicable to the Regulated Activity being conducted by an Authorised Person (e.g., Operating a Multilateral Trading Facility, Providing Custody or Dealing). COBS Rule 17.1.2 operates as a 'sign-post' Rule designed to draw the attention of Authorised Persons conducting a VA Regulated Activity to the fact that they must comply with all Rules applicable to Authorised Persons, including:

a) all other relevant chapters of COBS;

b) the General Rulebook ("GEN");

c) the Anti-Money Laundering and Sanctions Rulebook ("AML");

d) the Islamic Finance Rulebook; and

e) the Code of Market Conduct ("CMC").

20) The table below sets out the main risk areas, and the related mitigations for each of these risk areas, under the Virtual Asset Framework.

RISK		MITIGANT
1.	**AML/CFT/ SANCTIONS/TAX**	The AML Rulebook applies in full to all Authorised Persons. Authorised Persons also need to consider their reporting obligations in relation to FATCA and the Common Reporting Standard.
2.	**CONSUMER PROTECTION**	All material risks associated with Virtual Assets generally, Accepted Virtual Assets and an Authorised Persons' products, services and activities must be appropriately disclosed, and monitored and updated on an ongoing basis.

3.	**TECHNOLOGY GOVERNANCE**	Systems and controls must be in place in relation to: • Virtual Asset wallets; • Private keys; • Origin and destination of Virtual Asset funds; • Security; and • Risk management and systems recovery.
4.	**'EXCHANGE-TYPE' ACTIVITIES**	Multilateral Trading Facilities (MTFs) using Virtual Assets are required to have in place, among other things, the following: • Market surveillance; • Fair and orderly trading; • Settlement processes; • Transaction recording; • A rulebook(s); • Transparency & public disclosure mechanisms; and • Exchange-like operational systems and controls.
5.	**CUSTODY**	Virtual Asset Custodians are subject to Chapter 15 (read together with Rule 17.8) and Chapter 16 of COBS. Frequent reconciliations and reporting of Virtual Assets, as well as appropriate internal controls to safeguard them, are required.

21) An Authorised Person that carries on a Regulated Activity other than a VA Regulated Activity is not generally required to seek FSRA approval in respect of the use of Virtual Assets as part of that Regulated Activity or to comply with Chapter 17 of COBS. The FSRA retains the discretion to impose certain requirements outlined in Chapter 17 of COBS as conditions on such an Authorised Person's FSP, where the FSRA deems it necessary to mitigate risks associated with that Authorised Person's business model.

Combination of Regulated Activities

22) Applicants approved by the FSRA as an Authorised Person and permitted to conduct a VA Regulated Activity will be granted an FSP for the relevant Regulated Activity. An Applicant seeking to conduct activities in relation to Specified Investments / Financial Instruments, in addition to Virtual Assets, will need to apply to the FSRA to be able to do so, and will need to comply with the FRSA's requirements in relation to those Specified Investments / Financial Instruments.[6]

[6] Subject to paragraph 142 which notes that an Authorised Person Operating a Multilateral Trading Facility that also wishes to be authorised as a Recognised Investment Exchange ('RIE') must relinquish its FSP in order to obtain a Recognition Order with a stipulation allowing the RIE to Operate a Multilateral Trading Facility.

FSRA powers in respect of Virtual Assets

23) Authorised Persons conducting VA Regulated Activities should note that the FSRA has broad powers under section 5A and 5B of FSMR. The FSRA has additional powers in relation to Recognised Bodies. For example, the FSRA has powers to require an Authorised Person to either take such action as the FSRA may specify, or cease the conduct of a Regulated Activity in respect of a Virtual Asset, for such period of time as the FSRA thinks appropriate.

REGULATORY REQUIREMENTS FOR AUTHORISED PERSONS ENGAGED IN REGULATED ACTIVITIES IN RELATION TO VIRTUAL ASSETS

Conducting a Regulated Activity in relation to Virtual Assets

24) Chapter 17 of COBS applies to all Authorised Persons conducting a VA Regulated Activity, requiring compliance with all requirements set out in COBS Rules 17.1 to 17.6. Authorised Persons that are Operating a Multilateral Trading Facility or Providing Custody in relation to Virtual Assets are also required to comply with the additional requirements set out in COBS Rules 17.7 and 17.8 respectively.

Accepted Virtual Assets

25) COBS Rule 17.2.1 provides that an Authorised Person conducting any VA Regulated Activity shall not conduct such Regulated Activity with a Virtual Asset which is not an Accepted Virtual Asset. An Authorised Person is obliged to assess each Virtual Asset it proposes to use against the criteria outlined in COBS Rule 17.2.2 to determine whether that Virtual Asset meets the FSRA's requirements for an Accepted Virtual Asset. It is also required to notify the FSRA upon completion of that assessment no later than five Business Days prior to using the Virtual Asset.[7]

26) Prior to assessing a particular digital asset against the criteria outlined in COBS Rule 17.2.2, an Authorised Person must carefully consider the definition of 'Virtual Asset' and confirm that the relevant asset satisfies that definition.

27) An Authorised Person should note that the guidance below in paragraphs 28 to 36 relates only to the assessment of a Virtual Asset against the FSRA's requirements for an Accepted Virtual Asset. An Authorised Person should also engage with its FSRA supervision team to ascertain whether there are any other requirements to be met prior to the launch of the proposed Virtual Asset. This may include, for example, changes or updates to an Authorised Person's public facing documentation (including its rules, client agreement and/or terms of use, risk disclosures etc.), its operational requirements (including surveillance, custody,

[7] Authorised Persons should note that Accepted Virtual Assets approved for use by the FSRA under the previous FSRA-led approval process retain their Accepted Virtual Asset status for such Authorised Persons without the need for formal assessment or notification to the FSRA. Such Accepted Virtual Assets must be included on the list of Accepted Virtual Assets published by the Authorised Person on its website and are subject to the ongoing monitoring requirement outlined in COBS Rule 17.2.6.

transaction monitoring and other systems, policies and procedures) and/or any other relevant regulatory matters (including conduct or otherwise).

Guidance on governance arrangements in respect of assessing Virtual Assets

28) For the purposes of making and submitting an assessment under COBS Rule 17.2, an Authorised Person should ensure that it has suitable and robust governance arrangements in place to effectively assess, and continuously monitor, that the Virtual Assets recognised, or proposed to be recognised, as Accepted Virtual Assets by the Authorised Person comply with the requirements set out in COBS Rule 17.2. The FSRA expects that an Authorised Person's governance arrangements will be proportionate to its nature, scale and complexity and will be properly documented and adhered to. For example, larger Authorised Persons should consider establishing a dedicated committee and associated process, while smaller Authorised Persons may consider it appropriate for its review to be conducted through its relevant key functions (e.g. compliance, risk management, information technology, operations etc). Such governance arrangements should clearly define responsibilities for decisions relating to the change in use of Accepted Virtual Assets by an Authorised Person, including adding, suspending/halting or removing a Virtual Asset from being offered as part of a VA Regulated Activity.

29) Authorised Persons should engage with the FSRA for the purpose of implementation of these governance arrangements. These arrangements should also be reviewed periodically by the relevant key functions within the Authorised Person, with such reviews and findings properly documented and available for review by the FSRA, as required.

30) Authorised Persons should establish and maintain suitable record keeping arrangements, including comprehensive documentation and accurate records related to both initial and ongoing Virtual Asset assessments, including supporting evidence, relevant notifications submitted to the FSRA, and client communications and disclosures.

Accepted Virtual Asset assessment criteria

31) A Virtual Asset that meets the FSRA's requirements, as demonstrated by an individual Authorised Person, will constitute an Accepted Virtual Asset for that Authorised Person only. COBS Rule 17.2.2 states that, for the purpose of determining whether a Virtual Asset meets the requirements of being an Accepted Virtual Asset, an Authorised Person must adequately assess the following criteria:

a) Traceability/monitoring: whether Authorised Persons are able to demonstrate the origin and destination of the specific Virtual Asset, if the Virtual Asset enables the identification of counterparties to each transaction, and if on-chain transactions in the Virtual Asset can be adequately monitored;

b) Security: whether the Virtual Asset is able to withstand, adapt, respond to, and improve on its specific risks and vulnerabilities, including relevant factors and risks relating to its use, including testing, maturity, and ability to allow the appropriate safeguarding of secure private keys;

c) Market profile: the duration that the Virtual Asset has been in existence, the sufficiency, depth and breadth of market demand, the proportion of the Virtual Asset that is in circulation, the controls/processes to manage potential volatility of such Virtual Asset and any sanctions and adverse media in respect of the parties associated with the Virtual Asset, including founders, contributors, foundation members, investors and key decision-makers. This extends to establishing whether there is any association of the Virtual Asset with illegal activities or any serious concerns that its use may circumvent sanctions restrictions;

d) Exchange connectivity: whether there are exchanges that support the Virtual Asset; the jurisdictions of these exchanges and whether such exchanges are suitably regulated;

e) DLT infrastructure and ecosystem: whether there are issues relating to the underlying blockchain's consensus mechanism, its security and/or usability of the DLT used for the purposes of the Virtual Asset; including whether the Virtual Asset leverages an existing DLT for network and other synergies, and, in the case of a new DLT, whether the new DLT has been demonstrably stress tested;

f) Innovation / efficiency: whether the Virtual Asset demonstrates utility by, for instance, helping to solve a fundamental problem, addressing an unmet market need or creating value for network participants; and

g) Practical application / functionality: whether the Virtual Asset possesses quantifiable functionality.

32) In preparing an assessment for a Virtual Asset, the FSRA expects Authorised Persons to conduct a risk-based, comprehensive, and objective assessment. This assessment should include the criteria outlined in COBS Rule 17.2.2 as elaborated upon in paragraph 33 below.

33) An Authorised Person should consider the relative importance of each criterion taking into account all relevant considerations, including the Authorised Person's Regulated Activities and the nature of the Virtual Asset being assessed. The below provides further guidance on the application of certain of the assessment criteria outlined in COBS 17.2.2.

Assessment Criterion	**Guidance**
Traceability/monitoring	Authorised Persons should assess whether the Virtual Asset's origin and destination can be traced, whether flows can be analysed to establish risk exposures and whether on-chain activity can be effectively monitored through suitable Know Your Transaction (KYT) screening tools. At present, native blockchain explorers are generally not considered sufficient for monitoring and identification purposes. Particular attention should be given to Virtual Assets that incorporate privacy-enhancing features—such as ring signatures, stealth addresses, or similar mechanisms—

Assessment Criterion	Guidance
	that obscure sender and receiver details, as these Virtual Assets may significantly limit traceability and increase financial crime related risks. For Virtual Assets that offer optional privacy features, Authorised Persons must assess whether these features materially impact traceability and whether effective monitoring remains possible. Authorised Persons should implement appropriate policies, procedures, systems and controls to identify transactions using optional privacy features, explicitly restrict such transactions, and clearly inform clients that any inbound transfers made using privacy-enhancing mechanisms will be treated as irretrievable, similar to the treatment of transfers sent to incorrect wallet addresses. Virtual Assets that enforce non-traceability by default are unsuitable and should not be offered to clients.[8]
Security	Authorised Persons should evaluate the security and resilience of a Virtual Asset based on its underlying technology, risk profile and any vulnerabilities specific to its design. A risk-based approach should be applied, considering the nature of the Virtual Asset and its issuance model: • for Virtual Assets issued via smart contracts – Authorised Persons should ensure that the smart contracts—or standardised programs through which they are deployed—have undergone an independent security review (conducted by a non-conflicted person) with adequate scope and coverage; • for Virtual Assets not governed by smart contracts, such as native protocol assets, Authorised Persons should evaluate factors, such as the robustness of the issuance process and the reliability of the underlying infrastructure, that is, the DLT itself. Where relevant, Authorised Persons should also assess additional security measures, such as bug bounty programs, past security incidents, and the track record of the Virtual Asset's development team. Consideration should also be given to the potential impact of security

[8] See section 5A(4) of FSMR, which prohibits the carrying on of a Regulated Activity in ADGM involving the issue, sale, purchase, transfer or custody of a Virtual Asset which is a privacy token, or any digital asset employing similar technology.

Assessment Criterion	Guidance
	breaches, loss of funds, operational disruptions, and any other adverse events that could affect the Virtual Asset or its ecosystem. The level of active developer activity in maintaining the underlying infrastructure or protocol and the speed and quality of response to exploited vulnerabilities should also be assessed.
Market Profile	Authorised Persons should consider significant lifecycle events that could influence the Virtual Asset's risk profile. These events may include the Virtual Asset's pre-launch status, any rebranding efforts, mergers or acquisitions involving the Virtual Asset or its project, and major protocol upgrades.
DLT infrastructure & ecosystem	Authorised Persons should identify the DLT on which the Virtual Asset operates and assess not only its security, consensus mechanism, and reliability, but also other factors such as its governance structure, decentralisation (such as node distribution), and the broader ecosystem. If a Virtual Asset is issued on a newer or less established DLT, Authorised Persons should ensure the technology has undergone sufficient evaluation and risk assessment, paying particular attention to factors such as past forks, network upgrades, known vulnerabilities, and any history of security incidents. A Virtual Asset issued on multiple DLTs may have varying risk profiles depending on each chain's security and reliability. Authorised Persons should assess the Virtual Asset within the context of the specific DLT on which it is used and evaluate risks from cross-chain bridges or interoperability protocols, such as bridge vulnerabilities and single points of failure. Additionally, Authorised Persons should consider broader ecosystem risks, including the Virtual Asset's generation process—such as minting, locking, wrapping, bridging, or algorithmic issuance—as well as its role in lending markets, staking rewards, and vesting schedules. These factors may introduce risks like centralisation in staking, liquidity constraints in lending, or inflationary pressures from token emissions. Wrapped and bridge-based tokens, as well as liquid staking assets, may pose further vulnerabilities or single points of failure.
Practical application/functionality	Authorised Persons should categorise Virtual Assets based on their functionality, use cases, or meaning as part of the assessment process. Authorised Persons should consider whether the Virtual Asset demonstrates meaningful innovation, solves real-world problems, or

Assessment Criterion	Guidance
	addresses market needs by creating value for network participants. Not all Virtual Assets are designed for technological or economic innovation. Some, such as meme coins, represent cultural movements, community initiatives, or symbolic values tied to specific groups. Virtual Assets intended to start, sponsor or sustain projects that could cause harm, such as promoting illicit or illegal material, should not be considered Accepted Virtual Assets. Authorised Persons should assess that a Virtual Asset's actual functionality aligns with any claims made by its issuers or developer community. Misalignment between stated use cases and real-world application may signal elevated risks or misrepresentation.

Process for notifying the FSRA

34) Following completion of its assessment of a VA, an Authorised Person seeking to use a new Virtual Asset should complete and submit to its FSRA supervision team the form entitled '*Notification to the FSRA of assessment of Virtual Asset for Accepted Virtual Asset status'*. This form must be submitted to the FSRA no later than five Business Days prior to the Authorised Person using the Virtual Asset.

Website publication requirement

35) Under COBS 17.2.6, an Authorised Person must maintain on its website a current list of the Accepted Virtual Assets it uses to conduct a Regulated Activity. Authorised Persons may wish to consider including a link to any relevant disclosures required under COBS Rule 17.6 on the same webpage as this list. The list should include the following information in respect of each Accepted Virtual Asset:

    a) the name and symbol of the Accepted Virtual Asset;

    b) the network on which it operates;

    c) where applicable, smart contract addresses; and

    d) any relevant trading or usage restrictions.

Continuous monitoring

36) An Authorised Person conducting a VA Regulated Activity in relation to an Accepted Virtual Asset must continuously monitor such Accepted Virtual Asset to ensure it continues to satisfy the criteria specified in COBS Rule 17.2.2. The FSRA expects that an Authorised Person's processes will include clear policies and procedures to address changes, whether

significant or not, which may affect how a particular Accepted Virtual Asset satisfies the criteria specified in COBS 17.2.2. These processes should encompass reporting to the FSRA where appropriate (noting applicable reporting obligations under GEN and COBS) and any action to be taken by the Authorised Person.

Capital Requirements

37) Except for an Authorised Person Operating an MTF using Virtual Assets, the capital requirements applicable to Authorised Persons conducting VA Regulated Activities are outlined in Chapter 3 of PRU and are generally aligned with those applicable to Authorised Persons conducting the same Regulated Activity in relation to traditional financial assets. However, the capital requirement for Authorised Persons Providing Custody in relation to Virtual Assets is the higher of a Base Capital Requirement of $250,000 or an Expenditure Based Capital Minimum ("EBCM") of six months' Annual Audited Expenditure ("AAE") (as compared to an ECBM of 18/52nd of AAE for an Authorised Person Providing Custody in relation to traditional financial assets). Where an Authorised Person is Providing Custody in relation to both traditional financial assets and Virtual Assets, the higher capital requirement applies.

38) The capital requirements applicable to an Authorised Person Operating an MTF are outlined in COBS 17.3, which cross-refers to MIR Rule 3.2. MIR Rule 3.2 requires such an Authorised Person to hold regulatory capital of:

    a) an amount equal to six months' operational expenses; plus

    b) unless the FSRA directs otherwise, an additional buffer amount of up to a further 6 months' operational expenses.

39) Pursuant to these Rules, regulatory capital must be held by an Authorised Person in fiat form. Operational expenses under MIR Rule 3.2 should be considered in accordance with the International Financial Reporting Standards (IFRS).

40) Operational expenses, as set out in MIR Rule 3.2.1, broadly includes all of the overhead, non-discretionary costs (variable and exceptional items can be excluded) incurred (or forecast to be incurred) by an Authorised Person in its operations over the course of a 12-month period. Technology-related operational expenses, such as the use of IT servers and technology platforms, storage and usage of IT equipment and technology services required for the overall operability of the Authorised Person's platform, are to be included. Development costs, such as research and intellectual property patenting can be excluded.

41) The FSRA may impose additional capital requirements on a particular Authorised Person where it considers that its regulatory capital requirement is insufficient to adequately address all relevant risks.

Anti-Money Laundering and Countering Financing of Terrorism

42) The use of Virtual Assets raises significant regulatory concerns for regulatory authorities and law enforcement agencies worldwide, particularly in relation to Money Laundering ("ML") and Terrorism Financing ("TF"). International bodies, such as the International Monetary Fund ("IMF"), the Financial Action Task Force ("FATF"), the Bank for International Settlements ("BIS") and the International Organisation for Securities Commissions ("IOSCO"), have issued different Digital Asset (including Virtual Asset and ICO) warnings to investors and market participants advising of the significant risks, including ML and TF risks, and the possibility of Digital Assets being used for wider illegal purposes.

43) FATF has identified certain key risks associated with Virtual Assets,[9] which include the following:

a) Digital Assets (including, in particular, Virtual Assets) may operate in an anonymous or pseudo-anonymous manner. Virtual Assets can be traded via Internet platforms, are generally characterised by non-face-to-face Client relationships, and may permit (pseudo-)anonymous funding and transfers (cash funding or third-party funding through 'virtual exchanges' that may not properly identify the source or destination of funds);

b) The global reach of Virtual Assets increases the potential for ML/TF risks. Virtual Asset systems can be accessed via the Internet (including via mobile phones), and can be used to make cross-border payments and fund transfers;

c) Virtual Asset platforms commonly rely on complex infrastructures utilising several entities, often spanning multiple countries, to transfer funds or execute payments. This segmentation of services means that responsibility for ML/TF compliance and supervision/enforcement may be unclear. Moreover, Client and transaction records may be held by different entities, in different jurisdictions, making it more difficult for regulators and law enforcement agencies to access them. These issues are exacerbated by the rapidly evolving nature of 'decentralised' technologies used by Virtual Asset businesses, including the changing number and types/roles of participants providing services in the Virtual Asset ecosystem; and

d) Components of the Virtual Asset system may be located in jurisdictions that do not have adequate ML/TF controls.

44) On 22 February 2019, FATF issued a public statement recognising the need to adequately mitigate the ML and TF risks associated with digital asset activities.[10] As per the statement, FATF proposed more details relating to the regulation and supervision/monitoring of virtual

[9] http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html

[10] Though the activities deemed by FATF as 'virtual asset activities' are wider, they do cover the activities deemed by FSRA as Virtual Asset activities. FATF uses the term 'virtual assets', which for the purposes of (and consistency within) this Guidance has been replaced with the term 'digital assets'.

assets ("VAs") and virtual asset services providers ("VASPs")[11] by way of its (Draft) Interpretive Note to Recommendation 15, "*New technologies*".

45) On 21 June 2019, FATF released a revised Guidance for a Risk-Based Approach (RBA) for VAs and VASPs, as well as an Interpretative Note for Recommendation 15. This built upon previous FATF statements by clarifying an RBA for Anti-Money Laundering and Countering the Financing of Terrorism ("AML/CFT") purposes.[12] The basic principle underlying the FATF Guidelines is that VASPs are expected to "identify, assess, and take effective action to mitigate their ML/TF risks" with respect to VAs.

46) Further, the purpose and scope of the FATF Guidance is to clarify and assist:

a) national authorities in understanding and developing regulatory and supervisory responses to VA activities and VASPs with particular regard to the application of a RBA to their activities;

b) in the supervision or monitoring of VASPs for AML/CFT purposes;

c) in the licensing or registration of VASPs based on an applicable jurisdiction's requirements, subject to effective systems for monitoring/supervision;

d) in developing preventive measures including customer due diligence, recordkeeping, and suspicious transaction reporting, among others;

e) in the implementation of sanctions and other enforcement measures, as well as international co-operation;

f) in understanding risk indicators that should specifically be considered in a VA context, in relation to the obfuscation of transactions or limitations relating to a VASPs' ability to identify customers; and

g) the private sector seeking to engage in VA activities in understanding their AML/CFT obligations and how they can effectively comply with these requirements.

47) The Key Interpretive Notes to Recommendation 15 include:

a) Digital assets being considered as "property", "proceeds", "funds", "funds or other assets", or other "corresponding value", requiring the application of relevant AML risk mitigation measures under the FATF Recommendations to digital assets and VASPs; and

b) Recommendations 10 to 21 being proposed to directly apply to VASPs, subject to the following proposed qualifications/requirements:

[11] For the purposes of this Guidance, VASPs, though a wider collection of entities, are treated similar to Authorised Persons conducting a Regulated Activity in relation to Virtual Assets.
[12] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

i. Recommendation 10 – The occasional transactions designated threshold above which VASPs are required to conduct CDD is USD/EUR 1,000[13]; and

ii. Recommendation 16 – New requirements relating to the obligations of Originating VASPs and Beneficiary VASPS.

48) In order to develop a robust and sustainable regulatory framework for Virtual Assets, FSRA is of the view that a comprehensive application of its AML/CFT framework should be in place, including full compliance with, among other things, the:

a) UAE AML/CFT Federal Laws, including the UAE Cabinet Resolution No. (10) of 2019 Concerning the Executive Regulation of the Federal Law No. 20 of 2018 concerning Anti-Money Laundering and Combating Terrorism Financing;

b) UAE Cabinet Resolution 20 of 2019 concerning the procedures of dealing with those listed under the UN sanctions list and UAE/local terrorist lists issued by the Cabinet, including the FSRA Anti-Money Laundering and Sanctions Rulebook ("AML Rules") or such other AML rules as may be applicable in ADGM from time to time; and

c) adoption of international best practices (including the FATF Recommendations).

49) Taking into account Virtual Asset ML and TF risks, the importance of meeting global transparency and beneficial ownership standards, and the need to have proper mechanisms to exchange information with other regulators and counterparties, the FSRA requires that its AML Rules apply to all Authorised Persons, including those engaged in conducting a Regulated Activity in relation to Virtual Assets.

Key considerations for AML/CFT compliance

50) When considering the FATF Recommendations, in combination with the application of the AML Rules, the FSRA notes the following key principles that an Authorised Person conducting a Regulated Activity in relation to Virtual Assets should consider:

Principle 1: Risk-Based Approach

a) FATF expects countries, regulators, financial institutions and other concerned parties to adopt a 'Risk-Based Approach' ("RBA"). Authorised Persons are expected to understand the risks associated with their activities and allocate proper resources to mitigate those risks. A RBA can only be achieved if it is embedded into the compliance culture of the Authorised Person, which enables the Authorised Person to make decisions and allocate appropriate resources in the most efficient and effective way.

b) Authorised Persons should, on a periodic basis, carry out a proper risk-based assessment of their processes and activities. In order to implement the RBA,

[13] The FATF agreed to lower the threshold amount for VA-related transactions to USD/EUR 1 000, given the ML/TF risks associated with, and the cross-border nature of, VA activities.

Authorised Persons are expected to have processes in place to identify, assess, monitor, manage and mitigate ML risks. The general principle is that in circumstances where there are higher risks of ML, Authorised Persons are required to implement enhanced measures to manage and mitigate those risks.

c) One of the most challenging risks facing financial institutions is how the on-boarding of an Authorised Person may affect its relationship with foreign correspondent financial institutions, as well as the views of the regulator of those foreign correspondent financial institutions. In essence, a foreign correspondent financial institution relationship is built on the effectiveness of a financial institution's ML compliance program and ongoing monitoring capabilities.

d) With the use of cryptology and blockchain technologies at a nascent stage within financial services, any financial institution banking an Authorised Person must not only satisfy itself, but also its foreign correspondent financial institution(s), that the Authorised Person is well regulated and has appropriate systems and controls in place to address ML, TF and sanctions risks. These systems and controls should include robust processes to carry out CDD on Clients and beneficial owners, to monitor transactions for these risks, and the willingness and ability of the Authorised Person to provide complete transparency to its financial institution(s) and foreign correspondent financial institution(s) if and when required.

Principle 2: Business Risk Assessment

e) Chapter 6 of the AML Rules requires Relevant Persons to take appropriate steps to identify and assess the ML risks to which their businesses are exposed, taking into consideration the nature, size and complexity of their activities. When identifying and assessing these risks, several factors should be considered, including an assessment of the use of new technologies. Importantly, in the context of Virtual Assets, FATF Recommendation (15) states that:

"*Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.*"

f) Another aspect of assessing the business risk relevant to Authorised Persons is gaining familiarity with the characteristics and terminology[14] of the Virtual Asset industry. Additionally, Authorised Persons, and their management and staff, should be aware of the possible misuse of Virtual Assets in criminal activities, as well as the

[14] Examples of Digital Asset/Virtual Asset relevant terminology include: cold, warm or hot wallets/storage, on/off ramps, tainted wallets, public key, private key and forks.

technical and complicated nature of Virtual Assets (and the platforms they operate on).

g) When making its assessment, an Authorised Person must give consideration to all business risks. For example, while an issue may be identified in relation to cyber security (e.g., when dealing with hot wallets or using cloud computing to store data – being a 'technology' risk), the FSRA expects Authorised Persons to consider these risks from all perspectives to establish whether the risk triggers other issues for consideration (including ML/TF risks, technology governance and consumer protection). An Authorised Person must then use the identified risks to develop and maintain its AML/CTF policies, procedures, systems and controls and take all reasonable steps to eliminate or manage such risks.

Principle 3: Customer Risk Assessment and Customer Due Diligence

h) The FSRA expects all Authorised Persons to have fully compliant Client on-boarding processes. Virtual Assets have been criticised by regulatory bodies globally due to their (pseudo-)anonymity features, which makes tracking Client records and transactions more challenging for compliance officers and money laundering reporting officers.

i) Customer Risk Assessment and 'Customer Due Diligence' ("CDD") policies and procedures are required to be implemented by all Authorised Persons. Authorised Persons should have a process to assess and rate all their Clients according to that Client's risk profile (and taking into consideration the Authorised Persons' RBA). This risk-based assessment is required to be undertaken for each Client prior to transacting any business on behalf of the Client. Authorised Persons must undertake CDD for each Client and comply in full with Chapter 8 of the AML Rules noting that the FSRA does not consider it appropriate for Authorised Persons to use simplified CDD when conducting a Regulated Activity in relation to Virtual Assets, largely due to issues surrounding the (pseudo-) anonymity of Clients and transactions associated with Virtual Assets.

j) In the case of non-face-to-face on-boarding and ongoing due diligence of Clients who are natural persons, the FSRA expects that an Authorised Person will develop appropriate policies to ensure that the Client's identity is duly verified in accordance with all applicable Laws and Rules. This may include obtaining a "selfie" or by conducting a "liveness test". Irrespective of the method employed, it should validate that the individual being on-boarded is present during the on-boarding process, matches the individual in the identity documentation, and that the ID presented is valid and authentic. It should also include obtaining and authenticating a valid form of the Client's facial ID, which should be either the Client's passport with all applicable details clear and, or the original version (front and back) of an official government issued document, such as a national ID or driver's license. For the purposes of residents of the UAE, the primary form of documentation used should be the Client's Emirates ID card.

k) The FSRA understands that Authorised Persons may need to use new technology to improve Client on-boarding processes for the purpose of assessing and managing ML and TF risks. For example, in order for Authorised Persons to conduct non-face-to-face on-boarding they will need to implement facial recognition software to validate the "selfie" against the other uploaded documentation, or other suitable biometric technology.

l) The FSRA further understands that the proper use of such technologies (e.g., fingerprinting, retinal/eye scans, use of real-time video conference facilities to enable facial recognition) can assist with mitigation of the ML/TF risks associated with the use of Virtual Assets. Technological features, such as secure digital signatures that allow the verification of a Client's identity through a signed document, may also be acceptable to the FSRA. In all cases, an Authorised Person should ensure that the use of these technologies will not lead to a simplified process where the required Customer Risk Assessment and CDD requirements are not appropriately undertaken by an Authorised Person.

m) The FSRA recommends that Authorised Persons obtain a signed self-certification from their Clients identifying the details of all passports issued and held in their name(s). Authorised Persons may also use this as an opportunity to capture all tax related details in order to meet their international tax reporting obligations. Self-certification should not prevent Authorised Persons from conducting proper CDD.

Principle 4: Governance, Systems and Controls

n) Authorised Persons are required to implement an appropriate governance structure, especially in relation to Information Technology governance[15], and provide for the development and maintenance of all necessary systems and controls to ensure appropriate ML and TF compliance.

o) The FSRA expects that Authorised Persons may seek to utilise (their own or third-party) technologies and solutions to meet their regulatory obligations (e.g., customer risk assessment, detection of fraud, and transaction identification, monitoring and reporting) and risk management requirements (e.g., margin limits, large exposure monitoring).

p) The FSRA expects Authorised Persons to develop, implement and maintain effective transactional monitoring systems to determine the origin of a Virtual Asset and to monitor its destination, and to apply strong "know your transaction" measures which enable Authorised Persons to have complete granular data centric information about the transactions done by a Client.

q) The FSRA expects Authorised Persons to act responsibly and always be vigilant in ensuring that their activities are not subject to any misuse by participants transacting with Virtual Assets that may have been tainted in any way from an illegal activity. The FSRA expects that an Authorised Person's internal processes establish the types of 'indicators' or activities that could be used to identify when Accepted Virtual Assets

[15] Please also refer to the section on Technology Governance and Controls in this Guidance .

may have been used in an illegal manner. An Authorised Person should have a process for the management of when such 'indicators' (for example, certain Client or use of "mixer" and "tumbler" services) are triggered.

r) While the FSRA cannot recommend particular vendors or providers, all technology solutions must be fit for purpose and Authorised Persons should consider using those with an established track record and undertake their own due diligence/risk assessment to ensure competency and capability. The FSRA recognises that many of the (technology) solutions appropriate for mitigating Virtual Asset risks are continuing to be developed within the Virtual Asset industry itself.

s) The FSRA expects Authorised Persons to develop, implement and adhere to a "Virtual Asset Compliance Policy", tailored to meet specific Virtual Asset business compliance requirements, and reflecting a clear comprehension of the Authorised Person's understanding of its compliance responsibilities. The FSRA expects this policy to be well defined, comprehensive, robust and as specific to an individual Authorised Person's activities as possible. The policy can be separate or part of other compliance policies/manuals.

t) Following the development of the Virtual Asset Compliance Policy, Authorised Persons' compliance officers are expected to establish a "Virtual Asset compliance monitoring program", requiring internal reviews to be conducted in an efficient way, and on a periodic basis.

u) Authorised Persons must appoint a Money Laundering Reporting Officer ("MLRO") who will be responsible for the implementation and oversight of the Authorised Person's compliance with the AML Rules. Consistent with the FSRA's expectation in relation to all other Authorised Persons, an MLRO should have an appropriate level of seniority and independence to be effective in the role.

Principle 5: Suspicious Activity Reporting obligations

v) Authorised Persons should familiarise themselves with their reporting obligations under the AML Rules, in particular in relation to the reporting of suspicious activities/transactions.

w) Prior to commencing operations, the FSRA expects Authorised Persons to establish online connectivity with the UAE's Financial Intelligence Unit for the purposes of submitting Suspicious Activity Reports ("SARs"). Instructions on how to do this can be found on the FSRA's FCPU webpage.

x) Authorised Persons are required to establish sophisticated transaction monitoring systems to detect possible ML and TF activities. Systems should also be implemented to effectively identify any attempt to breach domestic and international sanctions. Such systems may rely on new technological solutions (including monitoring algorithms or Artificial Intelligence ("AI")).

Principle 6: Record keeping

y) As proper documentation is one of the main pillars of ensuring AML/CFT compliance, Authorised Persons are required to have policies and procedures in place to ensure proper record keeping practices. It is expected that an Authorised Person will maintain up to date records in accordance with the CDD obligations applicable to it and be prepared to provide the records upon request from the FSRA.

z) The FSRA understands that the transaction recording of many Virtual Asset transactions is linked to, or based on, DLT. This requires an Authorised Person to implement specific arrangements to ensure that, at a minimum, the Authorised Person and the FSRA have access to all relevant information as necessary. An Authorised Person may use a distributed ledger to store its data, provided it is able to provide this data, in an easily accessible format, to the FSRA when required.

aa) The FSRA views Virtual Asset activities that are linked to cash transactions as posing higher ML and TF risks, due to the source of funding being significantly more difficult to determine. Authorised Persons wishing to conduct cash transactions will be required to implement enhanced controls to mitigate the inherent risks of such transactions. Such controls may include, among other things, setting appropriate limits on cash deposits (e.g., daily, monthly, yearly limits), a prohibition on receiving cash directly, prohibitions on the receipt of cash other than from bank accounts, and prohibitions on receiving funds from third parties. In all cases, Authorised Persons will need to clearly demonstrate to the FSRA how their controls suitably mitigate the risks of cash transactions within their operations. Considering the wider consumer protection implications, the FSRA also considers it unlikely to be appropriate for Authorised Persons to accept deposits by way of credit card or credit facilities/credit lines.

bb) FSRA expects all Authorised Persons to exercise due care, to the utmost extent possible, in their day-to-day operations and when dealing with Clients or potential Clients. An Authorised Person's activities are expected to comply with the AML Rules, ensuring that their activities do not pose a regulatory risk or reputational damage to the ADGM Financial System.

International Tax Reporting Obligations

51) COBS Rule 17.4 requires Authorised Persons to consider and, if applicable, adhere to their tax reporting obligations including, as applicable, under the Foreign Account Tax Compliance Act ("FATCA"), set out in the Foreign Account Tax Compliance Regulations 2022 and the Common Reporting Standard, set out in the ADGM Common Reporting Standard Regulations 2017.

Technology Governance and Controls

52) While the FSRA adopts a technology-neutral approach to the regulation of Authorised Persons, Virtual Asset technology is widely considered to be in its early years of development and usage at scale. While it does not seek to regulate Virtual Asset technologies directly, the FSRA expects Authorised Persons to meet particular requirements in terms of their technology systems, governance and controls.

53) Historically, Virtual Asset business failures have often arisen as a result of the lack of adequate technology-related procedures, including, for example, lack of security measures, systems development methodologies, limited system penetration testing for operating a robust business and lack of technical leadership and management. The FSRA has therefore included specific Guidance regarding expected controls and processes to help mitigate these issues.

54) GEN Rule 3.3 requires an Authorised Person to establish systems and controls to ensure its affairs are managed effectively and responsibly, and to ensure such systems and controls are subject to continuous monitoring and review. COBS Rule 17.5 sets out additional requirements for appropriate technology governance and controls specific to Authorised Persons, with a focus on:

a) Virtual Asset Wallets;

b) Private and Public Keys;

c) Origin and destination of Virtual Asset funds;

d) Security; and

e) Risk Management.

55) When complying with GEN Rule 3.3 and COBS Rule 17.5, Authorised Persons should have due regard to the following key areas from a technology perspective:

a) Careful maintenance and development of systems and architecture (e.g., code version control, implementation of updates, issue resolution, and regular internal and third party testing);

b) Security measures and procedures for the safe storage and transmission of data;

c) Business continuity and Client engagement planning in the event of both planned and unplanned system outages;

d) Processes and procedures specifying management of personnel and decision-making by qualified staff; and

e) Procedures for the creation and management of services, interfaces and channels provided by or to third parties (as recipients and providers of data or services).

Maintenance and development of systems

56) Authorised Persons are expected to have a well-defined, documented and deliberate approach for the implementation and upgrade of systems and software.

57) Authorised Persons should also have well-established policies and procedures for the regular and thorough testing of any system currently implemented or being considered for

use (e.g., upgrades to a matching engine or opening of a new Application Programming Interface ("API") internally or with a third party).

58) The updated system should be tested for technical, operational and security vulnerabilities including but not limited to functional, penetration and stress testing. The outcome of the testing should be well structured and documented and signed off by the responsible (technology-focused) executives of the Authorised Person.

59) All changes made to the codebase in use are to be tracked and recorded, with a clear audit trail for appropriate internal checks and sign-off. The use of a version control system which allows for the accurate timestamping and identification of the user responsible for relevant changes should be considered.

60) Authorised Persons should maintain a clear and comprehensive audit trail for system issues internally, including security issues and those with third parties, their resolution and implementation of fixes.

61) Authorised Persons should conduct at least annual third-party verification/audit of core systems being used (including, if relevant, verification / audit of custody arrangements and verification of the amount of their purported holdings of Virtual Assets and Client Money). MTFs using Virtual Assets and Virtual Asset Custodians should have an annual review of their infrastructure undertaken by reputable third-party cyber security consultants, producing a list of recommendations and areas of concern.

Security measures and procedures

62) Authorised Persons should have measures and procedures in place which comply with network security industry best practices (e.g., the implementation of firewalls, strong passwords, password management procedures, multifactor authentication and encryption of data in transit and at rest).

63) Updates and patches to all systems, particularly security systems, should be performed as soon as safely feasible after such updates and patches have been released, whether these systems have been developed internally or developed by a third-party.

64) An Authorised Person's IT infrastructures (particularly for MTFs using Virtual Assets and Virtual Asset Custodians) are expected to provide strong layered security and seek the elimination of "single points of failure". IT infrastructure security policies are required to be maintained, describing in particular how strong layered security is provided and how "single points of failure" are eliminated. This includes, but should not be limited to, systems and procedures to limit the access of a single user to the use of private and confidential information of Clients.

65) IT infrastructures should be strong enough to resist, without significant loss to Clients, a number of scenarios, including but not limited to: accidental destruction or breach of data, collusion or leakage of information by employees/former employees, successful hack of a cryptographic and hardware security module or server, or access by hackers of any single set of encryption/decryption keys that could result in a complete system breach.

66) Authorised Persons should have in place policies and procedures that address information security for all personnel. The security policy should set the security tone for the whole entity and inform personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. To mitigate "key person risk", Authorised Persons are to ensure that there is no single individual that holds privileged or sensitive information that is critical to the operation of the Authorised Person.

67) The strong encryption of data, both at rest and in transit, should be included in the security policy. In particular, encryption and decryption of Virtual Asset private keys should utilise strong encryption protocols and algorithms that have broad acceptance with cyber security professionals. Critical cryptographic functions such as encryption, decryption, generation of private keys, and the use of digital signatures should only be performed within cryptographic modules complying with the highest, and internationally recognised, applicable security standards.

68) All security incidents and breaches should be logged and documented in detail as soon as practicable and the resolution and implementation details should subsequently be added to the log.

69) The use of open source software should be governed by clear, well documented and transparent rules and procedures governing the software's stability, security and fitness for purpose. Any open-source software, whether it is a compiled distribution or code, should be thoroughly tested for security and operational vulnerabilities. This testing should be signed off by the responsible executives of the Authorised Person before being used for the processing or storing of operational and Client information.

70) All APIs that are internal or external facing should be secured by strict access management procedures and systems, including encryption of the information (e.g., SSL certificates). All API access activity should be logged and scanned for security breaches on an ongoing basis.

71) All access management and credential changes (for employees, third-party service providers and Clients) should be governed and monitored by strict and well documented rules and procedures. This should include, but not be limited to, enforcing strong passwords and the monitoring of IP geo-location, use of VPN, TOR or unencrypted web connections.

Cryptographic Keys and wallet storage

72) The ability to send and receive Virtual Assets by recording new transactions on a distributed ledger is usually dependent on cryptographic keys – a public key and one or more private keys. The public key allows other users on a distributed ledger to send Virtual Assets to an address associated with that public key. The private key(s) provides full control of the Virtual Assets associated with the public key. As such, Authorised Persons need to have robust procedures and protective measures to ensure the secure offline generation, storage, backup and destruction of both public and private keys for their own wallet operations and where they offer wallet services to Clients.

73) Whether private keys are held on network attached devices or devices that are offline, Authorised Persons must have policies and procedures to ensure that they are not compromised by malicious actors.

Password protection and encryption

74) Authorised Persons should consider the use of multi-signature wallets (e.g., where multiple private keys are associated with a given public key and a subset of these private keys, sometimes held by different parties, are required to authorise transactions). Where a multi-signature solution is not feasible due to the underlying structure of the Virtual Asset, a similar mechanism or procedure should be in place (e.g., a multi-user authentication prior to enacting on-chain changes to the Virtual Asset holdings).

75) Authorised Persons should have clear policies and procedures that detail procedures for recovery in the event that a Client loses access credentials. These policies and procedures should also cover the recovery or re-generation of lost private keys (e.g., using a seed phrase if applicable).

76) Authorised Persons must have policies and procedures in place that set out actions and responsibilities in the event of a breach of private and public keys, as well as Client user access credentials.

Origin and destination of Virtual Asset funds

77) Virtual Asset transactions between public addresses take place on public DLT. Although it is normally possible to identify the public addresses of the parties to a transaction, it is often very difficult to establish the owner (whether natural or legal) of these addresses. This makes Virtual Assets attractive to money launderers, terrorist financers and other criminals.

78) The US Office of Foreign Asset Control (OFAC) has issued a statement requiring wallet addresses known to belong to individuals listed on the Specially Designated Nationals and Blocked Persons sanctions ("SDN") list to be reported. Further information is available on the OFAC website.[16] Additionally, there are companies collecting "tainted" wallet addresses that have been used in hacks, "dark web" transactions and other criminal activities.

79) An Authorised Person must have clear policies and procedures, consistent with the AML Rules applicable to it, to identify the source of funds and to ensure its compliance with COBS Rules 17.5(c) (Origin and destination of Virtual Asset funds) and 17.5(e) (Risk Management). These policies and procedures should cover due diligence on the deposits and withdrawals by legal persons that represent further multiple deposit-holders or withdrawal recipients of the Virtual Assets. For such deposits and withdrawals, Authorised Persons should be able to assess the ultimate beneficiaries' wallet addresses and their source or destination of funds as appropriate.

[16] https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx

80) It is crucial that Authorised Persons perform due diligence on their Clients before opening an account so that wallet addresses can be identified as belonging to a specific user. If a transaction is detected that originates from or is sent to a "tainted" wallet address belonging to a known user, that user should be reported. Authorised Persons should maintain lists of tainted wallet addresses and, if not in possession of their own services, utilise third party services to help identify such addresses.

81) Currently, there are technology solutions developed in-house and available from third party service providers which enable the tracking of Virtual Assets through multiple transactions to more accurately identify the source and destination of these Virtual Assets. It is expected that Authorised Persons may need to consider the use of such solutions and other systems to adequately meet their anti-money laundering, financial crime and know-your-customer obligations under the Virtual Asset Framework.[17]

Planned and Unplanned system outages

82) Authorised Persons should have a programme of planned systems outages to provide for adequate opportunities to perform updates and testing. Authorised Persons should also have multiple communication channels to ensure that its Clients are informed, ahead of time, of any outages which may affect them.

83) Authorised Persons should have clear, publicly available, procedures articulating the process in the event of an unplanned outage. During an unplanned outage, Authorised Persons should be able to rapidly disseminate key information and updates on a frequent basis.

Management of personnel and decision making

84) Authorised Persons should implement processes and procedures concerning decision making and access to sensitive information and security systems.

85) A clear audit log of decision making should be kept. Staff with decision-making responsibilities should have the adequate expertise, particularly from a technological standpoint, to make such decisions.

86) Protective measures should be implemented to restrict access to critical and/or sensitive data to key personnel only. This includes both digital and physical access. Authorised Persons should have processes and procedures to track and monitor access to all network resources. Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimising the impact of a data compromise. The maintenance of logs allows thorough tracking, alerting, and analysis when issues occur.

Third party outsourcing

87) Authorised Persons may use third party services for their systems. However, when doing so, an Authorised Person (pursuant to GEN Rule 3.3.31) retains full responsibility from a

[17] For full details on these obligations, please refer to the earlier section of AML/CFT.

regulatory perspective for any issues that may result from the outsourcing including the failure of any third party to meet its obligations. The FSRA requires that certain core systems (for example, the matching engine of an MTF using Virtual Assets) are maintained by the Authorised Person itself and will not generally permit these to be outsourced.

88) In its assessment of a potential third party service provider, an Authorised Person must satisfy itself that the service provider maintains robust processes and procedures regarding the relevant service (including, for example, in relation to the testing and security required in this section on Technology Governance).

89) In all circumstances, including in relation to business activities that are outsourced, an Authorised Person is expected to maintain a strong understanding of the third-party service being provided and, for critical services, have redundancy measures in place where appropriate.

90) Public and private cloud service providers should be subject to thorough screening. A set of well-defined and documented access management procedures should be in place. All service level agreements should be reviewed annually for serviceability and security of the systems and related operations as per the IT policies of the Authorised Person. A 'clear roles and responsibilities matrix' should be in place to delineate operations of a service provider from those of an Authorised Person. Physical access to systems should be limited to the relevant personnel and access should be monitored by the Authorised Person on an ongoing basis.

91) Authorised Persons are required to retain and be in the position to retrieve the data held on a cloud platform for such duration as they are required to under ADGM/FSRA record keeping purposes, and submit the data held on a cloud platform to the FSRA, as and when directed to do so, with immediate effect.

92) Authorised Persons who employ cloud-based data storage services for the purpose of recording personal data must also take into consideration ADGM data protection regulations. Consideration must be given to the jurisdiction within which the cloud storage service provider is located, or alternatively other arrangements which may facilitate compliance with applicable data protection requirements.

Forks

93) Authorised Persons should ensure that changes in the underlying protocol of a Virtual Asset that result in a fork are managed and tested proactively. This includes temporary forks which should be managed for reverse compatibility for as long as required.

94) Authorised Persons should ensure that their Clients are able to deposit and withdraw Accepted Virtual Assets in and out of an Authorised Person's infrastructure as and when requested before and after a fork (except during go-live). Clients should be notified well in advance of any periods of time when deposits and withdrawals are not feasible.

95) Where the underlying protocol of a Virtual Asset (e.g., the native token of that protocol) is changed, and the new version of that Virtual Asset is backwards-compatible with the old

version (soft fork), Authorised Persons should ensure that the new and old versions of the Virtual Asset continue to satisfy the relevant Accepted Virtual Asset requirements.

96) Where the underlying protocol of an Accepted Virtual Asset is changed, and the older version of the Accepted Virtual Asset is no longer compatible with the new version and/or there is an entirely new and separate version of the Virtual Asset (hard fork), Authorised Persons should ensure that client balances on the old version are reconciled with the new version of the Virtual Asset. Authorised Persons should also maintain transparent lines of communication with their Clients on how Authorised Persons are managing Clients' Virtual Asset holdings in such a scenario.

97) In the case of a hard fork, Authorised Persons should proactively manage any discrepancy between the balances recorded on the previous version versus the new version by engaging with the community which is responsible for updating and supporting the underlying protocol of the relevant Virtual Asset. Additionally, Authorised Persons should ensure that, where they seek to offer services in relation to the Virtual Asset associated with the new version of the underlying protocol, this new Virtual Asset meets the requirements for an Accepted Virtual Asset and that they notify the FSRA well in advance of offering the Virtual Asset as part of its activities.

Virtual Asset Risk Disclosures

98) Given the significant risks to Clients transacting in Virtual Assets, Authorised Persons conducting VA Regulated Activities are required to undertake a detailed analysis of the risks and have processes in place that enable them to disclose, prior to entering into an initial transaction, all material risks to their Clients in a manner that is clear, fair and not misleading. As this disclosure obligation is ongoing, and given the rapidly developing market for Virtual Assets, Authorised Persons are required to continually update this analysis and the resultant disclosures to its Clients to reflect any updated risks relating to:

a) the Authorised Person's products, services and activities;[18]

b) Virtual Assets generally; and

c) the specific Accepted Virtual Asset.

99) The FSRA expects that the disclosures to be made by an Authorised Person in order to satisfy COBS 17.6 may include:

[18] These disclosures should cover any specific arrangements, or lack of arrangements, for any product, service and activity of an Authorised Person. For example, in relation to custody of Clients' Virtual Assets, where an Authorised Person allows/requires Clients to self-custodise their Virtual Assets, this must be fully disclosed to Clients upfront, and Clients must be informed that the Authorised Person is not responsible for custody and protection of Clients' Virtual Assets. Where an Authorised Person is outsourcing part or all of the custody arrangements to a third party, this should also be disclosed to Clients.

a) Virtual Assets not being legal tender or backed by a government;

b) the values, or process for valuation, of Virtual Assets, including the risk of a Virtual Asset having no value;

c) the volatility and unpredictability of the price of Virtual Assets relative to Fiat Currencies;

d) that trading in Virtual Assets may be susceptible to irrational market forces;

e) that the nature of Virtual Assets may lead to an increased risk of Financial Crime;

f) that the nature of Virtual Assets may lead to an increased risk of cyber-attack;

g) there being limited or, in some cases, no mechanism for the recovery of lost or stolen Virtual Assets;

h) the risks of Virtual Assets being transacted via new technologies, (including distributed ledger technologies ('DLT')) with regard to, among other things, anonymity, irreversibility of transactions, accidental transactions, transaction recording, and settlement;

i) that there is no assurance that a Person who accepts a Virtual Asset as payment today will continue to do so in the future;

j) that the nature of Virtual Assets means that technological difficulties experienced by the Authorised Person may prevent the access or use of a Client's Virtual Assets;

k) any links to Virtual Assets related activity outside ADGM, which may be unregulated or subject to limited regulation; and

l) any regulatory changes or actions by the FSRA or a Non-ADGM Regulator that may adversely affect the use, transfer, exchange, and value of a Virtual Asset.

The FSRA is of the view that merely restating this non-exhaustive list of risks, either in its application or in the risk disclosures to its Clients, does not satisfy an Authorised Person's risk disclosure requirements.

100) For the purposes of interpreting the reference to "initial Transaction" in COBS Rule 17.6, Authorised Persons can meet the obligation in this Rule at any time prior to the 'initial Transaction'. For example, the introduction of a new Accepted Virtual Asset to trading on an MTF may require a further specific risk disclosure being made to Clients of the MTF in relation to the risks of trading in that new Accepted Virtual Asset (as assessed by the MTF).

101) The FSRA will need to understand the process by which an Authorised Person will communicate the risks outlined in COBS Rule 17.6.2, as well as any other relevant material risks to its Clients. Where the Clients of an Authorised Person are required to enter into a

Client Agreement, the Authorised Person may make its first such risk disclosure in that Client Agreement.

102) Considering the heightened inherent risks associated with investing in Virtual Assets and the FSRA's objective of providing a regulatory regime that offers adequate consumer protection, the FSRA is of the view that all Authorised Persons should, prior to on-boarding a Client, ensure that the services, or new services, proposed to be provided to a Client are appropriate, taking into account such matters as the Client's relevant knowledge, experience and investment objectives. Where a conflict between the inherent risks and the appropriateness for a Client is identified, the Authorised Person should take all reasonable steps to resolve such a conflict.

Market Abuse, Transaction Reporting and Misleading Impressions (FSMR)

103) As the Virtual Asset Framework does not treat Virtual Assets as Financial Instruments / Specified Investments, certain FSMR provisions have been expanded to specifically capture the use of Virtual Assets within ADGM.

104) Importantly, the Market Abuse Provisions in Part 8 of FSMR specifically cover Market Abuse Behaviour in relation to Accepted Virtual Assets admitted to trading on an MTF. In this regard, the FSRA imposes the same high regulatory standards to Accepted Virtual Assets traded on MTFs as it does to Financial Instruments traded on Recognised Investment Exchanges, MTFs or OTFs in ADGM.

105) Similar to the reporting requirements imposed on Recognised Investment Exchanges and MTFs in relation to Financial Instruments, MTFs (pursuant to FSMR Section 149) are required to report details of transactions in Accepted Virtual Assets traded on their platforms.[19] The FSRA expects MTFs using Virtual Assets to report to the FSRA on both a real-time and batch basis.

106) In addition, FSMR provisions on Misleading Statements apply to Accepted Virtual Assets. The FSRA expects that all communications (including advertising or investment materials or other publications) made by an Authorised Person will be made in an appropriate manner and that an Authorised Person conducting a Regulated Activity in relation to Virtual Assets will implement suitable policies and procedures to comply with the requirements of FSMR.

107) The FSRA continues to consider developments to its regulatory perimeter in the context of its Market Abuse provisions, including for the purposes of any future determination of whether the provisions ought to be extended to further capture Virtual Asset trading activity that is not specifically linked to trading on an MTF. In this context, and particularly in the case of intermediary-type Authorised Persons, the FSRA reminds such Authorised Persons of their wider responsibilities under the Virtual Asset Framework in relation to the use of

[19] The additional obligation of an MTF using Virtual Assets to undertake its own market surveillance is set out in paragraph 136 (d) of this Guidance.

Virtual Assets, including in relation to client risk disclosures, suitability and best execution (see paragraphs 98-102, 108(a) and (b) and 114).[20]

SPECIFIC FSRA GUIDANCE ON THE VIRTUAL ASSET FRAMEWORK

Application of particular Rules in COBS

108) The Rules referenced in COBS Rule 17.1.4 apply to all Transactions undertaken by an Authorised Person conducting a VA Regulated Activity. The Rules referenced in COBS Rule 17.1.4 are as follows:

a) COBS Rule 3.4 (Suitability);

b) COBS Rule 6.5 (Best Execution);

c) COBS Rule 6.7 (Aggregation and Allocation);

d) COBS Rule 6.10 (Confirmation Notes);

e) COBS Rule 6.11 (Periodic Statements); and

f) COBS Chapter 12 (Key Information and Client Agreement)).

109) These requirements are relevant to the concept of 'Investment Business' within COBS and can be considered more relevant to certain Authorised Persons, particularly those that are 'dealing' in Accepted Virtual Assets. The FSRA understands that some of these obligations may not apply to all Authorised Persons (particularly MTFs using Virtual Assets).

Protection of Client Money

110) An Authorised Person that conducts a VA Regulated Activity and which holds or controls Client Money must comply with all the relevant Client Money rules in Chapter 14 of COBS (read together with COBS Rule 17.8). Under COBS Rule 17.8.4, such Authorised Persons are required to carry out reconciliations of Client Money in Client Accounts as follows:

a) Reconciliations with respect to COBS Rule 14.11.1 shall be carried out at least every week; and

b) Reconciliations with respect to COBS Rule 14.11.4 shall be carried out within five days of the date to which the reconciliation relates.

Substance requirements of Authorised Persons

111) An Authorised Person conducting a VA Regulated Activity must commit resources of a nature allowing it to be operating in substance within ADGM. Depending on the relevant

[20] This is particularly relevant when intermediary-type Authorised Persons trade into other unregulated/lightly regulated markets globally. FSRA expects Authorised Persons to have suitable controls (including client protection controls and disclosure mechanisms) in place for such activity.

Regulated Activities being undertaken, the FSRA expects to see substantive resources committed within ADGM across all lines of the Authorised Person's activity, including, but not limited to, commercial, governance, compliance/surveillance, operations, technical, IT and HR functions. The FSRA expects the 'mind and management' of an Authorised Person to be located within ADGM. Further discussion on substance in relation to MTFs using Virtual Assets is set out at paragraph 131.

Virtual Asset Brokers or Dealers

112) Authorised Persons intending to operate solely as a broker or dealer for Clients (including the operation of an OTC broking or dealing desk) are not permitted to structure their broking / dealing service or platform in such a way that would have it be considered as operating a market / MTF using Virtual Assets. The FSRA would consider features such as allowing for price discovery, displaying a public trading order book (accessible to any member of the public, regardless of whether they are Clients), and allowing trades to automatically be matched using an exchange-type matching engine as characteristic of an MTF using Virtual Assets, and not activities acceptable for an intermediary-type Authorised Person to undertake.

113) An Authorised Person that only has an FSP to operate as a broker / dealer (in relation to Virtual Assets) and not as an MTF is required to design and structure its operations, user interface, website, marketing materials and any public or client-facing information such that it does not create the impression that it is running an MTF. In practice, this may include not displaying any publicly-accessible information that may appear like a trading order book, not providing for any price discovery, and not giving actual or potential Clients the impression that they are interacting with an MTF.

114) Virtual Asset brokers / dealers are required to comply with the best execution requirements in COBS Rule 6.5 at all times.

115) Virtual Asset brokers / dealers are required to disclose the following information to Clients:

a) How they execute and route Client's orders and source liquidity (e.g., whether they pass or route orders to other brokers, dealers or exchanges to execute). Where a broker / dealer routes Client orders to a single liquidity source such as an MTF for execution, it must also disclose this to all Clients;

b) Whether it may carry out proprietary trading on its own account, and if so, whether it may trade against Clients' positions;[21]

c) The fees it charges Clients; and

d) How it determines the prices of the Accepted Virtual Assets it quotes to Clients.

[21] The FSRA would not allow Virtual Asset brokers / dealers to "front run" or trade ahead of Clients' trades, or trade on a proprietary basis alongside Clients' trades.

Appointment of advisers

116) Applicants should consider the appointment of compliance advisers, with the appropriate skills, knowledge and experience (taking into account the activities that the Applicant is proposing to undertake), to provide the requisite assistance to the Applicant throughout the Application process. The FSRA expects that Applicants should engage its compliance advisers by no later than when it begins to prepare its Application and should retain them up until the date of operational launch.

Certain class order modifications / waivers

117) The FSRA appreciates that some Rules, in particular within MIR and parts of COBS, may not apply to certain Authorised Persons and the FSRA may grant class order modification and waiver relief in relation to these Rules.[22] To the extent that an Applicant or Authorised Person considers that any other Rules do not apply to it by virtue of its business model or otherwise, the FSRA expects that an application for modification or relief be submitted either as part of its Application or at such later date as the relief may be required.

Data protection obligations for Authorised Persons

118) ADGM's data protection regime protects individuals' right to privacy by controlling how personal information is used by organisations and businesses registered in ADGM. All entities registered in ADGM that hold or process the personal data of an individual must protect personal data in compliance with the ADGM Data Protection Regulations 2021 (the "Data Protection Regulations"). Specifically, an Authorised Person, as a data controller, will be responsible for determining the purposes for which, and the manner in which, personal data is processed in compliance with the Data Protection Regulations. Failure to do so risks enforcement action and compensation claims from individuals, each of which are considered data subjects under the Data Protection Regulations.

119) Data controllers must ensure that personal data which they process is:

a) processed fairly, lawfully and securely;

b) processed for specified, explicit and legitimate purposes in accordance with the data subject's rights and not further processed in a way incompatible with those purposes or rights;

c) adequate, relevant and not excessive in relation to the purposes for which they are collected or further processed;

d) accurate and, where necessary, kept up to date; and

[22] Any such relief, and the terms on which it is based, is located at https://en.adgm.thomsonreuters.com/rulebook/waivers-and-modifications-0

e) kept in a form, which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data were collected or for which they are further processed.

120) Data controllers must, on request, provide individuals with access to any personal information they hold.

121) The registration of all data controllers with the ADGM's Registration Authority[23] is mandatory. A data controller must maintain records of all personal data processing operations undertaken by it or on its behalf and must notify the Registration Authority upon becoming aware of any security breach involving personal data as soon as possible.

122) Personal data must not be transferred to a country or territory outside ADGM unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data. The Registration Authority has designated certain jurisdictions as providing an adequate level of protection; a current list is maintained by the Registration Authority upon its website, which may be updated from time to time.

123) If an Authorised Person intends to transfer personal data to a recipient, including by way of storage of personal information upon a cloud based service or remote server, located in a jurisdiction other than those considered by the Registration Authority to be possessing adequate safeguards, such transfer is only possible under certain conditions, including, but not limited to, circumstances where the:

a) individual has consented to the proposed transfer;

b) proposed transfer is necessary for the performance of the service for which the data controller was engaged by the individual; and

c) data controller and data processor have entered into an approved form of agreement concerning the protection of personal data, or the Registration Authority has granted a permit consenting to the proposed transfer.

Transactions with unknown counterparties

124) Authorised Persons should avoid a transactional interaction with any infrastructure or services where a counterparty is unknown or anonymous (e.g., via certain peer to peer or decentralised exchanges) at any stage of the process within and outside of the Authorised Persons' core operations. This is to ensure that Authorised Persons remain compliant with FSRA Rules at all times and do not unnecessarily expose their activities to risks emanating from tainted sources / destination of funds.

[23] Detailed information concerning data protection obligations under the ADGM data protection regime, including registration forms, fee information and specific guidance is available on the Registration Authority website.

125) Authorised Persons should also avoid inclusion of liquidity, pricing and settlement data from such entities in their day-to-day operations. Any interaction (whether deliberate or not) with such entities should be notified to the FSRA as soon as practicable.

Margin trading

126) An Applicant/Authorised Person wishing to provide margin trading to its Clients will need to submit for approval details of the terms upon which it proposes to do so (for an Applicant, in its Application – for an Authorised Person as part of ongoing supervisory arrangements). As a general position, the FSRA would only consider allowing Applicants/Authorised Persons with a relevant proven track record to provide margin trading.

127) Particular focus will be placed on an Applicant or Authorised Person's proposed leverage ratio. The FSRA is aware that some of the significant Virtual Asset markets around the world operate margin ratios of between 2-4 times, and it is likely that FSRA consideration of leverage ratios will be in reference to this position.

128) Applicants that are not proposing, or permitted, to carry out margin trading will have a restriction from doing so placed on their FSP.

Insurance

129) The FSRA recognises the growing interest/interplay between Virtual Asset activities and the provision of insurance to such activities. While recognising this, the FSRA does not require Authorised Persons to maintain insurance in relation to their Virtual Asset activities, as the provision of insurance is considered a second line of defence. However, the FSRA recommends that Virtual Asset brokers/dealers and Virtual Asset Custodians take out asset protection policies, which cover a minimum of hot wallets. As a first line of defence, the FSRA expects all Authorised Persons to ensure the proper structuring of their business operations and to implement robust mechanisms for the mitigation of actual and potential areas of risk.

MULTILATERAL TRADING FACILITIES AND VIRTUAL ASSETS

Background

130) The FSRA considers Operating a Multilateral Trading Facility to be a key VA Regulated Activity in ADGM.

Substance requirements for MTFs

131) Consistent with the treatment of all Authorised Persons, the FSRA requires MTFs to be based in substance within ADGM. In addition to the substantial commitment of resources required of an MTF Operator, this also means that the FSRA's regulatory oversight of an MTF extends to its order book, matching engine, rulebook(s), ensuring fair and orderly markets, settlement, and for the purposes of preventing/monitoring for Market Abuse, amongst the relevant requirements set out in the Market Infrastructure Rulebook ("MIR") and COBS Chapter 8.

132) In practical terms, this means that for a start-up MTF, its entire order book and the functionality of its matching engine will be subject to FSRA oversight. For existing operational virtual asset exchanges that already have their order book / matching engine outside ADGM prior to making an application, a determination of which parts (if not all) of its order book (and how its matching engine) will come under FSRA regulatory oversight needs to be made by the Applicant,[24] to allow it to apply to become authorised as an MTF.

133) The FSRA is of the view that only MTFs can operate markets within ADGM that allow for the matching of orders, or for the purposes of price discovery, of Accepted Virtual Assets. For this reason, and the reasons set out above, the application of FSRA's regulatory oversight may, therefore, be distinctly different from other regulators globally.

Trading Pairs

134) The FSRA's expectation is that an MTF's primary trading pairs can only comprise of the following:

a) Fiat Currency (or other value) into Accepted Virtual Assets;

b) Accepted Virtual Assets into Fiat Currency (or other value); or

c) One Accepted Virtual Asset into another Accepted Virtual Asset.

Guidance in relation to Applicable Rules

135) In addition to the MTF Rules set out in COBS Chapter 8, MTFs are also required to meet the requirements set out in COBS Rules 17.1 to 17.6, and the additional Rules set out in COBS 17.7.[25]

136) Chapter 8 of COBS incorporates Rules from various other FSRA Rulebooks that must be complied with, including certain sections of MIR. COBS Rule 8.2.1 sets out various Rules in MIR that MTFs (using Virtual Assets) are required to comply with to the satisfaction of the FSRA, with the applicable Rules set out as follows:

a) MIR Rule 2.6 (Operational systems and controls): MIR Rule 2.6.1 requires an MTF to '*establish a robust operational risk management framework with appropriate systems and controls to identify, monitor and manage operational risks that key participants, other [MTFs], service providers (including outsourcees) and utility providers might pose to itself.'*

[24] In situations where an entity establishes an Authorised Person that routes orders to a virtual asset exchange outside ADGM (even as part of a Group that may be operating globally) instead of having orders matched within an MTF's order book within ADGM, that entity cannot obtain an MTF Exchange license within ADGM and can only be licensed as an intermediary-type Authorised Person within ADGM.
[25] Chapter 8 of COBS also contains the requirements for the operation of an Organised Trading Facility (OTFs). The application of OTF Rules, however, are not relevant to the operation of Virtual Assets.

i. In relation to systems and controls, the FSRA has provided guidance on what it expects in relation to technology governance controls in paragraphs 52 to 97 of this Guidance. The FSRA therefore requires an MTF to undertake its 'MTF' activities in compliance with these operational system and control requirements, in combination with the technology governance controls outlined earlier in this Guidance.

ii. The FSRA expects an MTF to undertake extensive due diligence and testing of its operational systems and controls, with the relevant reports of such testing capable of being provided to the FSRA for review. Such testing should be undertaken by an officer of the MTF possessing appropriate skills and experience. The testing reports need to confirm the robustness of the MTF's systems and address any potential areas of failure. Testing should include the settlement processes for the movement of Virtual Assets between wallets, and the general connectivity of the MTF's systems with other parties. Testing should be ongoing, building in processes for the introduction of new Accepted Virtual Assets.

iii. An MTF will need to provide policies and procedures that clearly evidence how it will effectively address a failure of its systems. Failures must be rectified as soon as practicable, with an MTF's business continuity plan including detailed and realistic response timeframes for failures or disruptions.

b) MIR Rules 2.7.1 and 2.7.2 (Transaction recording): FSRA expects that the primary ledger technology systems and controls of an MTF (whether they be DLT or multiple-ledger technologies) will be such that transaction recording and reporting is easily facilitated, and that all FSRA requirements can be effectively complied with. Where reconciliations are required to be undertaken, for example, between a DLT based ledger and an internal ledger maintained by an MTF for the purposes of transactions and/or settlement, the FSRA will need to be satisfied that the reconciliation process is robust, timely and efficient.

c) MIR Rule 2.8 (Membership criteria and access): MIR Rule 2.8.1 requires that an MTF *'must ensure that access to its facilities is subject to criteria designed to protect the orderly functioning of the market and the interests of investors'*.

Access Requirements

i. MIR Rules 2.8.2, 2.8.3, 2.8.5 and 2.8.6 support the operation of MIR Rule 2.8.1, and the FSRA expects that MTFs consider the application of the requirements across these Rules - for example, MIR Rule 2.8.5 contains substantive provisions that should apply, regardless of what model of 'access' an MTF (using Virtual Assets) utilises.

ii. The FSRA recognises, however, that MTFs (using Virtual Assets) generally operate an 'access' model that does not include Members[26] (e.g., access is

[26] To clarify, 'Members' are not the same as 'Institutional Clients'.

granted directly to (retail and institutional) Clients of the MTF). An MTF operating in this manner will, therefore, need to ensure that it has appropriate processes, controls and rules to 'protect the orderly functioning' of its market, its facilities and the interests of its investors.

iii. By not adopting a 'Member-access' model and allowing direct 'Client-access', MTFs lose one layer of regulatory/supervisory defense that Recognised Investment Exchanges and Member-access MTFs have, in that they do not have Members assisting them in the undertaking of the necessary due diligence and compliance reviews of investors being on-boarded into their market. The FSRA, in these circumstances, requires MTFs to undertake their own CDD reviews for every client accessing (trading on) their market (something which traditionally a Recognised Investment Exchange or Member-access MTF can rely on its Members to do). Resultant AML/CFT obligations therefore fall more directly on a Client-access MTF as well.

iv. The FSRA expects that the controls (and resultant resourcing needs) of an MTF be appropriately budgeted and accounted for, including specific controls for when it has Clients that are institutional Clients (as the current conventional Member/institutional client global regulatory model may not properly account for, and mitigate, the risks relevant to operating such model within the Virtual Asset space). For example, where an MTF has institutional Clients that are regulated as Authorised Persons (for example, an Authorised Person that is a broker / dealer) within ADGM, the MTF may take comfort from the fact that its Clients are appropriately regulated (including for AML purposes). An MTF may not, however, take such comfort when its institutional Clients may come from unregulated/less regulated jurisdictions. MTFs with an institutional Client base will therefore need to demonstrate how the MTF will adequately comply with the requirements of the AML Rulebook where its institutional Clients are trading on behalf of further clients.

v. Given the current lack of global regulation of Virtual Asset intermediaries, those MTFs operating a 'membership model' will need to assess whether their members are adequately regulated in their home jurisdiction, such that the MTF can suitably rely on their Members, for example, to undertake CDD/AML checks. Where members are not properly regulated, the FSRA expects that MTFs will centralise the relevant compliance activities internally (and not be able to rely on their 'members' for such purposes).

vi. Depending on the model, controls and criteria to be adopted by an MTF, the class order modification or waiver relief granted by the FSRA to Authorised Persons conducting VA Regulated Activities as referred to in paragraph 117 of the Guidance may apply.

Rulebook(s)

i. Further to MIR Rule 2.8, the FSRA expects an MTF to have a rulebook(s) in place. This rulebook should be clearly labelled as such and be publicly available on the website of the MTF.

ii. Supporting documents such as participation agreements, terms of business, product lists, user guides and technical specifications are also a key part of the operation of an MTF and should be consistent with its rulebook. The FSRA does not consider that the existence of these documents alone meets the requirement of having a transparent and effective rulebook. The FSRA considers it good practice that these supporting documents are available and transparent, alongside the published rulebook, to the extent possible.

iii. The content of a rulebook[27] should enable an MTF to demonstrate how it is complying with MIR Rule 2.8, be supported by procedures that are complete and clear, and all in support of an MTF seeking to ensure that behaviour within its market is fair and orderly.

iv. The FSRA expects MTFs to require explicit acknowledgement via a user agreement, that participants have read, understood and will abide by the rulebook at all times.

v. The FSRA expects an MTF to undertake regular reviews of its rulebook to ensure it is consistent with relevant regulatory and legislative requirements. Best practice may see such activity undertaken no less than every twelve-months.

d) MIR Rule 2.9 (Financial crime and market abuse): MTFs are required to operate an effective market surveillance program to identify, monitor, detect and prevent

[27] A non-exhaustive list of sections that the FSRA consider key for inclusion in a rulebook include:

- participant eligibility criteria;
- participant obligations;
- Accepted Virtual Asset eligibility criteria;
- Virtual Asset fork protocols;
- fair and orderly trading rules;
- AML and source of fund requirements;
- market abuse prohibition rules;
- measures to prevent a disorderly market;
- disciplinary procedures;
- pre- and post-trade obligations;
- settlement obligations;
- certain wallet and custody provisions;
- default provisions;
- compliance;
- monitoring & enforcement;
- definitions / glossary of terms;
- co-operation with regulators; and
- powers to amend rules and consultation procedures.

conduct amounting to market misconduct and/or Financial Crime. Given the significant risks, and the nascent nature and constant pace of development of the Virtual Asset industry, an MTF's surveillance system will need to be robust, and regularly reviewed and enhanced.

i. The FSRA recognises that an MTF outside ADGM may not be subject to a similar regulatory standard as that which applies within ADGM. The FSRA recommends, therefore, that MTFs spend the time to consider the application of MIR Rules 2.9.1 to 2.9.3, which technology, systems and controls they propose to use for these purposes, and the associated resourcing needs required to undertake these functions appropriately. For this reason, among others set out in this Guidance, the FSRA is of the view that it is not appropriate for an MTF to outsource its compliance / market surveillance functions.

ii. The FSRA further reminds MTFs, and investors trading on an MTF, of the Market Abuse provisions applicable to the trading of Accepted Virtual Assets on an MTF.[28]

e) MIR Rule 2.11 (Rules and consultation): To meet MIR Rules 2.11.1 to 2.11.11, an MTF must ensure that it has appropriate procedures in place for it to make rules, for keeping its rules under review, for consulting and for amending its rules. MIR Rule 2.11.2 requires proposed rule changes be subject to FSRA approval.

f) MIR Rule 3.3 (Fair and orderly trading): MIR Rules 3.3.1 to 3.3.4 establish the requirements an MTF must meet for providing fair and orderly trading across its market, and for having objective criteria for the efficient execution of orders. The FSRA considers these requirements to be fundamental to the operation of an MTF.

g) COBS Rule 8.3.1 & MIR Rule 3.7 (Public disclosure):

i. Any arrangements of an MTF used to make information public (including trading information required to be disclosed under COBS Rule 8.3.1) must satisfy a number of conditions, including that it is reliable, monitored continuously, and made available to the public on a non-discriminatory basis. While an MTF can choose the format structure to be used for dissemination, MIR Rule 3.7.4 requires it to conform to a consistent and structured format.

ii. In terms of the timing of disclosure of MTF trading information, the FSRA recognises that current virtual asset industry practice is for such trading information to be released on a real-time basis (in alignment with current practice for trading within spot commodity markets, but different to the current industry/regulatory practice of delayed data within certain securities/derivatives markets). The FSRA is not proposing any additional specific requirements at this stage (to those already applicable in COBS Rule 8.3.1 and MIR Rule 3.7) but will continue to monitor industry practice.

[28] Refer to paragraphs 103 to 107 of this Guidance.

h) MIR Rule 3.8 (Settlement and Clearing Services): An MTF will need to have clear processes in place for the settlement (and if applicable, the clearing) of all Accepted Virtual Asset transactions. As noted in the AML and Technology Governance sections of this Guidance, extensive stress testing on capabilities to connect successfully with third parties, and in relation to the movement of Accepted Virtual Assets between wallets, will be required to be undertaken to the FSRA's satisfaction. The FSRA will not necessarily require a connection to a separate Recognised (or Remote) Clearing House where the MTF can demonstrate that it has in place *'satisfactory arrangements for the timely discharge, Clearing and settlement of the rights and liabilities of the parties to transactions effected'* on the MTF, including where it is utilising the services of a Virtual Asset Custodian.

i) MIR Rule 3.10 (Default Rules): Depending on whether an MTF operates a 'Member-access' model or it allows direct 'Client-access' will determine the full, or partial, application of MIR Rules 3.10.1 to 3.10.3. The FSRA, at a minimum, expects MTFs to have in place both rules and a process to suspend or terminate access to its markets in circumstances where a Client/Member is unable to meet its obligations in respect of transactions relating to Accepted Virtual Assets.

   i. The FSRA suggests that an Applicant/Authorised Person consider different scenarios/circumstances where it may need to utilise the powers provided to it under its Default Rules, and take appropriate action as required. Scenario testing of this kind could relate to when there is a financial and/or technical 'default' in relation to, for example, its custody, fiat token or wider banking arrangements. Due to a prevalence of pre-funding of (client) positions within Virtual Asset markets, the impact of a 'default' in such a scenario may not necessarily be on a per-transaction basis, but could be structural in nature, in limiting the ability of Clients to fund their positions (and therefore the ability of the MTF to operate on a fair and orderly basis).

   ii. To prepare for the event of a loss/default, the FSRA expects an MTF to have, within its policies, a clear process for the management of such loss (e.g., what is the exposure of individual Clients, counterparties, its Custodian and itself, as applicable).

137) COBS Rule 17.7.4 specifies that certain notification requirements applicable to Recognised Investment Exchanges under MIR Rules 5.1, 5.3 and certain information requirements under MIR Rule 5.4.1 apply to MTFs (using Virtual Assets). These are additional requirements applicable to MTFs using Virtual Assets. MTFs using Virtual Assets will also need to comply with any other applicable notification requirements, including those set out in the Accepted Virtual Assets section of this Guidance in relation to the use of additional Accepted Virtual Assets.

138) It is recognised that MTFs may take varying approaches in relation to the custody of Virtual Assets. An MTF may use third party custodians but still be holding itself out to its Clients as being responsible for custody of their Accepted Virtual Assets. Alternatively, an MTF may provide custody of Clients' Accepted Virtual Assets wholly itself, done "in-house" without the use of any third-party custodians. An MTF whose custody arrangements fall into either of these two scenarios will also be considered to be Providing Custody of Virtual Assets for

the purposes of the Virtual Asset Framework and will be required to comply with COBS Chapters 15 and 16, and take guidance from the section below on "Authorised Persons Providing Custody of Virtual Assets".

139) As further set out in paragraphs 153 and 154, in circumstances where an MTF is also Providing Custody, the FSRA expects appropriate segregation of responsibilities, staff, technology and, as appropriate, financial resources, between the operations of the MTF and the Virtual Asset Custodian.

Recognised Investment Exchanges Operating an MTF using Virtual Assets

140) Pursuant to MIR Rule 3.4.1, a Recognised Investment Exchange may operate an MTF, provided that its Recognition Order includes a stipulation permitting it to do so. MIR Rule 3.4.2 requires that where such a stipulation is granted to a Recognised Investment Exchange, the Recognised Investment Exchange must meet the requirements of the Virtual Asset Framework in relation to operation of an MTF (using Virtual Assets) while the remainder of its operations must be operated in compliance with the MIR Rules.

141) This means that a Recognised Investment Exchange (in addition to operating markets relating to the trading of Financial Instruments (including Digital Securities) can, where permitted by the FSRA and subject to MIR Rule 3.4.2, operate a separate MTF, OTF and/or MTF using Virtual Assets under its Recognition Order.

142) Authorised Persons that are operating an MTF wishing to also operate a Recognised Investment Exchange will be required to relinquish their FSP upon obtaining a Recognition Order (to operate a Recognised Investment Exchange). If licensed by the FSRA to carry out both activities (e.g., operating an MTF and operating a Recognised Investment Exchange), the relevant Recognition Order will include a stipulation to that effect pursuant to MIR Rule 3.4.1 - see paragraph 140 above).

143) The FSRA appreciates that Applicants, Authorised Persons and Recognised Bodies may wish to build out their Regulated Activities in ADGM on a staggered basis. For example, an entity may wish to start out in ADGM as an MTF (using Virtual Assets) and migrate to other exchange/market infrastructure activities in due course. Equally, a Recognised Investment Exchange may wish to start out in the area of Derivatives or Digital Securities and then introduce Virtual Asset activities (as an MTF) in due course. The FSRA suggests that in such circumstances an Applicant reach out to discuss the steps for doing so as early as possible.

AUTHORISED PERSONS PROVIDING CUSTODY OF VIRTUAL ASSETS

144) Authorised Persons Providing Custody in relation to Virtual Assets ("Virtual Asset Custodians") provide the service of helping Clients safeguard their Accepted Virtual Assets. Virtual Asset Custodians include firms that solely offer the custody of Virtual Assets for Clients, as well as MTFs and other intermediaries who additionally provide the service of custodising Accepted Virtual Assets on behalf of Clients.

145) Similar to the approach taken in relation to activities undertaken by MTFs in relation to Virtual Assets, the FSRA considers the activities undertaken by Virtual Asset Custodians to

be a key VA Regulated Activity within ADGM. Accordingly, the Virtual Asset Framework contains specific additional requirements applicable to Virtual Asset Custodians.

146) Virtual Asset Custodians are required to comply with Chapter 15 (read together with COBS Rule 17.8) and Chapter 16 of COBS at all times. Virtual Asset Custodians are also required to comply with COBS Rules 17.1 to 17.6. Authorised Persons should also note that COBS 17.8.2 requires that "Investment" or "Investments", (and, a result, the corresponding references to "Client Investments") be read as encompassing "Virtual Asset" or "Virtual Assets", as applicable. This means that an Authorised Person that holds, controls, or Provides Custody for, Accepted Virtual Assets, on behalf of their Clients must comply with all relevant Safe Custody rules in Chapter 15 of COBS (read together with Chapter 17 of COBS) at all times. This approach has been taken by the FSRA to ensure that Accepted Virtual Assets are afforded the same protections as other similar products and activities under FSMR and the FSRA Rulebooks.

147) Under COBS 17.8.3, Virtual Asset Custodians are required to:

a) send out statements in respect of its holdings of a Client's Virtual Assets to Retail Clients at least monthly (as required under COBS Rule 15.8.1(a)); and

b) carry out all reconciliations of a Client's Virtual Asset holdings at least every week (as required under COBS Rule 15.9.1).

Custodial Arrangements for Clients' Virtual Assets

148) The FSRA notes that there are broadly three types of custodial arrangements over Accepted Virtual Assets that Authorised Persons are likely to adopt:[29]

a) **Type 1 (Custodial Wallet)**: The Authorised Person is wholly responsible for the custody of a Client's Accepted Virtual Assets and provides this service "in-house" through its own Virtual Asset wallet solution. Such an arrangement includes scenarios where an MTF provides its own in-house proprietary wallet for Clients to store any Accepted Virtual Assets bought through that exchange or transferred into the wallet from other sources. Type 1 also includes firms who solely provide the dedicated service of helping Clients (such as MTFs, broker-dealers, traders, fund / asset managers) custodise their Accepted Virtual Assets. The Type 1 custody provider effectively holds Virtual Assets (e.g., the private keys) as an agent on behalf of Clients and has control over these Accepted Virtual Assets.[30]

b) **Type 2 (Outsourced Custodial Wallet)**: The Authorised Person is wholly responsible for the custody of a Client's Accepted Virtual Assets but operationally outsources this function to a third-party Virtual Asset custodian. Type 2 arrangements include the

[29] The FSRA recognises that there may be other alternative Virtual Asset custody models in existence or which may emerge in future. Entities seeking to provide such alternative models and who are unsure of the regulatory obligations they may attract are encouraged to contact the FSRA as early as possible.

[30] Clients using such Type 1 custodial wallets do not necessarily have full and sole control over their Accepted Virtual Assets. In addition, there is a risk that should the custodial wallet provider cease operations or get hacked, Clients may lose their Accepted Virtual Assets.

scenario where an MTF uses a third party custody service provider to hold its Clients' Accepted Virtual Assets.[31]

c) **Type 3 (Non-Custodial / Self-Custody Wallet):** The Authorised Person allows/requires Clients to wholly "self-custodise" their Accepted Virtual Assets, and at no point does the Authorised Person have partial or full control over these Clients' Virtual Assets. The Type 3 custody provider is typically a third-party hardware or software company that offers the means for each Client to hold their Virtual Assets (and fully control private keys) themselves. Hardware wallets, mobile wallets, desktop wallets and paper wallets are generally examples of non-custodial wallets. Clients using non-custodial wallets have full control of and sole responsibility for their Virtual Assets, and the non-custodial wallet provider does not have the ability to effect unilateral transfers of Clients' Virtual Assets without Clients' authorisation.[32]

149) Entities seeking to operate either Type 1 or Type 2 custodial arrangements above would generally be regarded as carrying out the Regulated Activity of Providing Custody and require a FSP from the FSRA.

150) With respect to the Type 3 non-custodial wallets described above, the wallet provider is merely providing the technology; it is the wallet user who has full control of and responsibility for their Virtual Assets. Given they have no control over Clients' Virtual Assets, Type 3 non-custodial wallet providers would generally not be required to seek an FSP to Provide Custody. The FSRA considers the Type 3 scenario above, where Clients are required to self-custodise their Accepted Virtual Assets, as potentially posing a material risk given that the burden of protecting and safeguarding Virtual Assets falls wholly upon Clients, and that Virtual Assets face the constant risk of being stolen by malicious actors. As such, Authorised Persons requiring Clients to self-custodise Virtual Assets are required to disclose this fact fully and clearly upfront to Clients, and meet the disclosure standards elaborated in paragraphs 98 to 102 above. The FSRA will take the quality of these proposed disclosures into account when assessing applications from Authorised Persons proposing to require Clients to self-custodise their Virtual Assets.

Governance Arrangements for Virtual Asset Custodians

151) From a governance perspective, a Virtual Asset Custodian should have proper governance structures in place to avoid or mitigate actual or potential conflicts of interest between its custody functions and any other activities or functions within itself or with other Group entities. Such governance arrangements may include having a separate team, which does not have other conflicting responsibilities within the firm, handling custody.

[31] The Type 2 custody arrangement would include the scenario where an Authorised Person engages an external third-party Virtual Asset custody provider to safeguard / custodise Clients' Accepted Virtual Assets, but the Authorised Person is still designated as one of the multi-signature signatories required to "sign" or authorise the transfer of movement of Client's Accepted Virtual Assets. The Authorised Person still retains responsibility at all times to Clients for safeguarding their Accepted Virtual Assets.

[32] The Type 3 custody arrangements may include scenarios where some distributed MTFs require Clients to self-custodise their Accepted Virtual Assets. Such MTFs only provide the trading platform for Clients to buy and sell Accepted Virtual Assets. Clients are required to source and use their own third-party custody arrangements (which the distributed MTFs have no control over or responsibility for).

152) To assist with ring-fencing and to reduce potential conflicts of interest, an Applicant that wishes to Provide Custody in relation to Virtual Assets and concurrently provide other Regulated Activities should consider the merit of establishing a separate, standalone legal entity for its Virtual Asset Custodian activities.[33] If so established, this standalone entity would need to apply to the FSRA for its own FSP to carry on the Regulated Activity of Providing Custody.

Other Requirements Pertaining to the Provision of Custody of Virtual Assets

Governance

153) Authorised Persons operating as Virtual Asset Custodians must not, at any time, permit arrangements whereby just a sole party or signatory is able to completely authorise the movement, transfer or withdrawal of Accepted Virtual Assets held under custody on behalf of Clients. In particular, Authorised Persons must not have custody arrangements whereby only a sole person can fully access the private key or keys for the Accepted Virtual Assets held under custody by the Authorised Person. Preventing such arrangements can help reduce potential key person risk such as theft, fraud, unwillingness or inability of the sole party to grant access to private keys.

154) Authorised Persons are also required to mitigate the risk of collusion between all authorised parties or signatories who are able to authorise the movement, transfer or withdrawal of Accepted Virtual Assets held under custody. Authorised Persons are required to provide information on these mitigating controls to the FSRA.

155) Authorised Persons are required to maintain, at all times, an updated list of all past and present authorised persons who were / are able to view, initiate, authorise, sign, approve or complete the transfer or withdrawal of Accepted Virtual Assets held under custody on behalf of Clients. In addition, Authorised Persons are to have clearly defined policies and procedures to enable or revoke the authority granted to these persons.

156) Authorised Persons are required to have policies and procedures in place that clearly describe the process that will be adopted in the event that it knows or suspects that the Accepted Virtual Assets it is holding under custody on behalf for Clients has been compromised, such as in the event of a hacking attack, theft or fraud. Such policies and procedures should detail the specific steps the firm will take to protect Clients' Accepted Virtual Assets in the event of such incidents. Authorised Persons should also have the ability to immediately halt all further transactions with regard to the Accepted Virtual Assets.

Obligations in relation to outsourcing

157) Where an Authorised Person that operates or seeks to operate as a Virtual Asset Custodian wishes to outsource part or all of the custody function to a third party, the Authorised Person is required to perform its due diligence and background checks on the third party, and

[33] For example, a Virtual Asset Exchange may decide to offer a dedicated Accepted Virtual Asset custody service to certain Clients.

ensure that the third party meets all the FSRA's requirements applicable to Virtual Asset Custodians. Such Authorised Persons are required to make full disclosures to their Clients and to the FSRA regarding such outsourced custody arrangements. The Authorised Person retains full responsibility from a regulatory perspective for any issues that may result from such outsourcing, including the failure of any third party to meet its Virtual Asset Custody obligations.

Third party audit obligations

158) Authorised Persons should have independent third party verification or checks carried out at least annually to verify that the amount and value of Accepted Virtual Assets held on custody on behalf of Clients is correct and matches what the Virtual Asset Custodian is supposed to hold.

STABLECOINS

159) The FSRA has implemented a dedicated framework for the issuance of Fiat-Referenced Tokens ("FRTs") in ADGM. An FRT is a digital asset, the transfer and storage of which is achieved through the use of distributed ledger or similar technology, the purpose of which is to be used as a medium of exchange with a stable store of value, by:

a) referencing a fixed amount of a single fiat currency; and

b) enabling the holder to redeem the token in exchange for the amount of the fiat currency referred to in a) from its issuer upon demand.

160) COBS 17.2.1 also requires that an Authorised Person carrying on a Regulated Activity involving an FRT must only use Accepted FRTs (i.e., those which have been approved by the FSRA). Persons seeking to carry on a Regulated Activity involving FRTs, including those seeking to issue FRTs in ADGM, should consult relevant Rules and Guidance relating to FRTs, including Chapters 17 and 19A of COBS.

161) The FSRA recognises that not all assets described as 'stablecoins' will satisfy the definition of an FRT. For example, a 'stablecoin' may aim to maintain a stable value relative to an asset(s) other than a single fiat currency and so will not satisfy the definition of FRT.[34] Persons seeking to carry on a Regulated Activity involving an asset described as a 'stablecoin' but which does not satisfy the definition of an FRT should contact the FSRA to discuss the regulatory treatment of the specific asset in question.

NON-FUNGIBLE TOKENS

162) Non-fungible tokens ("NFTs") are cryptographic assets on a DLT with unique identification codes and metadata that distinguish them from each other. Unlike Virtual Assets, they

[34] While there is no universally agreed legal or regulatory definition of the term 'stablecoin', the Financial Stability Board has defined the term as "a crypto-asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets": Financial Stability Board, High-level Recommendations for the Regulation, Supervision and Oversight of Global Stablecoin Arrangements: Final Report, 17 July 2023: https://www.fsb.org/uploads/P170723-3.pdf.

cannot be replicated, thus cannot be traded or exchanged at equivalency. Essentially, therefore, NFTs operate similar to a collector's item but are digital instead of physical.

163) The FSRA recognises the growing relevance of NFT markets within the wider digital asset markets. While the FSRA is not proposing to establish a formal regulatory framework for NFTs at this point, it will continue to monitor industry, market and regulatory developments. The FSRA is, however, in certain circumstances only, open to NFT activities being undertaken within ADGM, but only by its regulated, and active, MTFs which are also authorised to Provide Custody in relation to Virtual Assets (a "MTF / Virtual Asset Custodian") where both of those Regulated Activities are conducted within ADGM. Firms conducting own account or proprietary investments in NFTs are allowed to do so within ADGM.

164) The FSRA's current position in relation to NFTs is therefore as follows:

a) Relevant MTFs / Virtual Asset Custodians should establish within their ADGM Group an unregulated, commercially licensed NFT entity (the 'NFT Entity'). The NFT Entity would primarily be used as the commercially focused entity used to engage with NFT issuers and market participants and would therefore be 'ring-fenced' from the MTF / Virtual Assets Custodian from a legal (and therefore liability, resources, and funding) perspective;

b) An NFT Entity is to outsource back to the MTF/Virtual Asset Custodian all client, trading, auction and custody activities; and

c) All NFT activities will be captured for KYC and AML/CTF purposes, as the AML rules within ADGM will apply to the NFT Entity and continue to apply as relevant to the MTF/Virtual Asset Custodian.

165) While the FSRA will allow these regulated MTF/Virtual Asset Custodian Groups to undertake certain NFT activities within ADGM, it is important to note the following:

a) NFTs themselves remain outside FSRA regulatory oversight;

b) the NFT Entity, and the MTF/Virtual Asset Custodian, will need to satisfy the FSRA of its approval process for, and the monitoring of, the Issuers, and third-party integrated registries of the NFTs (noting that an Issuer cannot be themselves, or part of their Group); and

c) NFTs should be transferred into the MTF for auction/trading purposes and to the Virtual Asset Custodian for custodial purposes, but if not the MTF/Virtual Asset Custodian would need to satisfy the FSRA that it has proper systems and controls in place. An MTF/Virtual Asset Custodian would therefore need to allow/onboard only suitable third-party NFT registries and relevant auction houses, outside of themselves.

APPLICATION PROCESS

166) Applicants seeking to become an Authorised Person conducting a VA Regulated Activity must be prepared to engage heavily with the FSRA throughout the application process. The application process is broadly broken down into five stages, as follows:

a) Due Diligence & Discussions with the FSRA team(s);

b) Submission of Formal Application;

c) Granting of In Principle Approval;

d) Granting of Final Approval; and

e) 'Operational Launch' Testing.

Due diligence and Discussions with FSRA team(s)

167) Prior to the submission of an Application, all Applicants are expected to provide the FSRA with a clear explanation of their proposed business model and to demonstrate how the Applicant will meet all applicable FSRA Rules and requirements. These sessions will also involve the Applicants providing a number of in-depth technology demonstrations, across all aspects of its proposed Virtual Asset activities. The FSRA generally expects these meetings, where possible, to take place between the Applicant and the FSRA in person. Given the complexity of the activities associated with the Virtual Asset Framework, it is likely that a number of meetings will need to be held between an Applicant and the FSRA before the Applicant will be in a position to submit a draft, then formal, application.

Submission of Formal Application

168) Following discussions with the FSRA, and upon the FSRA having reasonable comfort that the Applicant's proposed business processes, technologies and capabilities are at a sufficiently advanced stage, the Applicant will be required to submit a completed Virtual Asset Application Form, and supporting documents, to the FSRA[35]. The Applicant's supporting documents include the submission of a detailed launch plan reflecting each of the steps (referencing the full set of operational and regulatory requirements) that the Applicant will take to progress from Application phase, through IPA and FSP to launch. Payment of the fees applicable to the Application must also be made at the time of submission. The FSRA will only consider an Application as having been formally submitted, and commence its formal review of the Application, upon receipt of both the completed Application, detailed launch plan and the associated fees.

[35] The FSRA will make available to the Applicant an editable version of the Virtual Asset Application Form at the appropriate time. Other ancillary forms to be submitted include the Approved Person Status form (for appointing Controlled Functions such as the SEO and Licensed Directors).

Granting of In Principle Approval (IPA)

169) The FSRA will undertake an in-depth review of the Application, and supporting documents, submitted by an Applicant. The FSRA will only consider granting an IPA for an FSP to those Applicants that are considered able to adequately meet all applicable Rules and requirements. An Applicant will be required to meet all conditions applicable to the IPA prior to being granted with final approval and an FSP for the relevant Regulated Activity.

Granting of Final Approval (Financial Services Permission)

170) Subject to being satisfied that the Applicant has met all conditions applicable to the IPA, the FSRA will grant the Applicant with final approval for an FSP for the relevant Regulated Activity. Final approval will be conditional upon the FSRA being further satisfied in relation to the Applicant's operational testing and capabilities, and completion of a third-party verification of the Applicant's systems where applicable.

'Operational Launch' Testing

171) An Applicant (particularly an MTF (seeking to use Virtual Assets) and/or Virtual Asset Custodian) will only be permitted to progress to operational launch when it has completed its operational launch testing to the FSRA's satisfaction, including completion of third-party verification of the Applicant's systems, where applicable.

172) Noting the heightened risks associated with activities related to Virtual Assets, Authorised Persons will be closely supervised by the FSRA once licensed. Authorised Persons will be expected to meet frequently with the FSRA, will be subject to ongoing assessments and should be prepared to undergo thematic reviews from time to time.

Opening a bank account

173) Given the associated risks within the Virtual Asset space, the global banking sector is focusing on account opening requests from entities associated with Virtual Assets with increased scrutiny. The FSRA has engaged in extensive discussions with local and international banks for the purposes of providing an overview of the Virtual Asset Framework and the stringent authorisation requirements imposed on Applicants when applying to become an Authorised Person. It is intended that those banks with a risk appetite to bank Virtual Asset players will glean comfort from the regulatory oversight of the FSRA and the issuance of an IPA to entities demonstrating that they have a clear roadmap of development of their business towards final approval and issuance of an FSP. The process for approval for the opening of a bank account with local or international banks will typically include a full explanation and review of an Applicant's AML and Client on-boarding processes and procedures, as well as its ability to monitor the source and destination of funds, amongst other areas of its Virtual Asset activities.

FEES

174) The fees applicable to Authorised Persons conducting a VA Regulated Activity have been established in consideration of the risks involved in relation to Virtual Asset activities and

the supervisory requirements placed on the FSRA to suitably regulate these Authorised Persons and Virtual Asset activities in ADGM.

175) The FSRA's approach is to apply a single "add on" fee in respect of carrying on a VA Regulated Activity. This "add on" fee applies in addition to the fees (application and supervision) applicable to the Regulated Activities being conducted, or proposed to be conducted, by an Authorised Person or an Applicant (see FEES Rule 3.17).

176) For example, an Applicant that wishes to carry on the Regulated Activities of Dealing in Investments as unmatched Principal and of Arranging Deals in Investments, both in relation to Virtual Assets, will be subject to the following fee schedule at the application stage and thereafter as an Authorised Person.

Application	**Fees Rule**	**Fee (USD k)**
Dealing in Investments as unmatched principal	3.4.1	40
Arranging Deals in Investments	3.8.1(c) + 3.2.1	10
Virtual Assets activity	3.17.1(a)	*20*
Total		**70**

Supervision[36]	**Fees Rule**	**Fee (USD k)**
Dealing in Investments as unmatched principal	3.4.2	50
Arranging Deals in Investments	3.8.2(c) + 3.2.2	10
Virtual Assets activity	3.17.2(a)	*15*
Total		**75**

177) An MTF using Virtual Assets is also required to pay a trading levy to the FSRA on a sliding scale basis, payable monthly in USD (see FEES Rule 3.18 for further details).

178) Pursuant to FEES Rule 1.2.4, the FSRA may impose additional fees in circumstances where a 'substantial additional' regulatory burden is imposed on FSRA. The FSRA also has discretion to reduce or waive all or part of any fee where it considers it fair and reasonable to do so in a specific case. The FSRA recommends that Applicants/Authorised Persons discuss any questions relating to fees with the FSRA as early as practicable.

[36] Prorated for period from time of authorisation until end of first calendar year.