هيئة الأوراق المالية والسلع
SECURITIES & COMMODITIES AUTHORITY

United Arab Emirates

Guidelines
Regulation of Virtual Assets and Virtual Assets Services Providers



www.sca.gov.ae
Toll Free 800722823 الرقم المجاني
scauae sca.uae sca_uae

Table of Contents

Table of Contents

Introduction

1. Securities and Commodities SCA "SCA" issues these guidelines under The Cabinet Resolution No. (111) of 2022 Concerning the Regulation of Virtual Assets and their Service Providers "Cabinet Resolution", the Chairman of the SCA's Board of Directors' The Chairman of the SCA's Board of Directors Decision No. 13/R.M of 2021 regarding the Rulebook for Financial Activities and Adjustment Mechanisms (« Rulebook »), and The Chairman of the SCA's Board of Directors' Decision No. (26/Chairman) of 2023 on the Regulation of the Virtual Asset Platform Operator. They shall be read along with the referred resolutions.

2. These guidelines shall apply on:
   - Virtual assets VAs;
   - Virtual Assets Services Providers.

3. These guidelines specify SCA's approach to regulating the use of virtual assets as an investment instrument, if they are used in the state, with the exception of financial free zones. These guidelines shall apply to virtual asset platform operator ,safe custody of virtual assets financial consulting in virtual assets , managing portfolio of virtual assets, virtual assets broker, virtual assets dealer and any other activities licensed in the future by the SCA with regard to regulating virtual asset activities. These guidelines, together with resolutions issued by the Cabinet and resolutions issued by the SCA in relation to virtual assets, are referred to as the "Virtual Assets Framework".

4. These guidelines shall not be a comprehensive source of the SCA's policy on the exercise of its regulatory functions and powers. The SCA shall not bound by the requirements stipulated in these guidelines and may:
   - Impose additional requirements to address any specific risks that may arise in connection with the use of virtual assets;
   - Waive or modify any rules related to the Virtual Assets Framework, in its sole discretion, where appropriate.

5. Unless otherwise specified or the context requires otherwise, the terms mentioned in these guidelines shall have the same meaning as defined in the Cabinet Resolution and the Glossary of Terms contained in the Rulebook and the Chairman of the SCA's Board of Directors' Decision No. (26/Chairman) of 2023 on the Regulation of the Virtual Asset Platform Operator.

Overview

6. Technological innovation is transforming the financial services industry. The continued advancement of new technologies has provided opportunities to significantly change and disrupt financial services and other related activities globally. Advances in distributed ledger technologies ("DLT") have given rise to various types of digital assets, including cryptocurrencies/virtual assets to facilitate economic transactions or transfer of value.

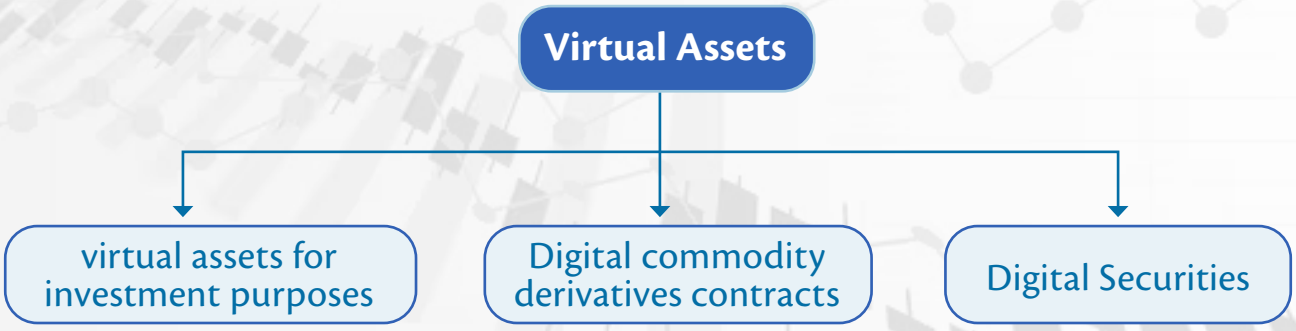
7. These guidelines focus primarily on the SCA's regulatory treatment of virtual assets, and the financial services activities that can be conducted in relation to virtual assets in the state excluding financial free zones. For the purposes of the Virtual Assets Framework, virtual assets are defined as follows:

   "Virtual Assets" means a digital representation of value that can be traded or digitally transferred and can be used for investment purposes, and does not include digital representations of paper currencies, securities or other money.

8. Virtual Assets are not issued or guaranteed by any regulatory body, and fulfill the above functions only by agreement within the community of Virtual Asset users.

9. As stated in the definition, virtual assets are divided into two parts, which are virtual assets for investment purposes and virtual assets for payment purposes. In this aspect, it must be noted that virtual assets for payment purposes, including stored value facilities, are subject to the jurisdiction of the Central Bank of UAE . This excludes virtual assets approved by the Central Bank for listing and trading for investment purposes on the virtual assets platform. Therefore, the reference to the term virtual assets in these guidelines means virtual assets for investment purposes wherever they mentioned.

10. The chart and table on the following pages illustrate the SCA's regulatory approach with respect to the digital asset classes that fall under its jurisdiction:



Virtual assets	Regulatory approach
Digital Securities	Although the digital security, or so-called securities based on distributed ledger technology (DLT-Securities), are in the form of an encrypted asset that can be traded or transferred digitally, it is considered a security subject to the legislations regulating traditional securities, taking into account any technological requirements imposed by the SCA from time to time as the case may be to enable proper use within a secure digital environment.
Digital commodity derivatives contracts	Although the digital commodity derivatives contracts are in the form of an encrypted asset that can be traded or transferred digitally, it is considered a security subject to the legislations regulating traditional securities, taking into account any technological requirements that the SCA may impose from time to time as the case may be to enable proper use within a secure digital environment.
virtual assets for investment purposes	It is considered a digital representation of value that can be traded or transferred digitally, and can be used for investment purposes, and does not include digital representations of fiat currencies, securities, or other funds. Although the SCA does not directly regulate mining operations and the issuance of virtual assets, virtual assets may not be traded except after they are included in the official list with a virtual assets platform operator licensed or registered with the SCA and after they are registered with the SCA in accordance with the terms and conditions for accepting virtual assets in accordance with the Appendix (1) By The Chairman of the SCA's Board of Directors' Decision No. (26/Chairman) of 2023 on the Regulation of the Virtual Asset Platform Operator.

11. For clarity, the Virtual Assets Framework shall not apply to:
    - Digital securities or digital commodity derivatives contracts.
    - Service tokens and non-fungible tokens that do not represent virtual assets for investment purposes.
    - Develop, deploy or use software for the purpose of mining, creating or extracting virtualassets.
    - Loyalty programs.
    - Virtual assets for payment purposes.
    - Any virtual assets evaluated by the SCA

Objectives of the Virtual Assets Framework

12. The virtual assets 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 facing regulatory bodies around the world. Without regulated entities controlling the creation and use of virtual assets, the system is open to significant financial crime and other risks. Therefore the virtual assets framework is considered comprehensive to effectively address the key risks posed by virtual asset trading. The SCA's view is that AML/CFT regulation alone will not sufficiently mitigate some of the broader risks related to virtual assets. Given the increased use of virtual assets as a means of investment and their connection to the mainstream financial system through virtual asset platforms, brokers, custodians and portfolio management, there is an increased potential for risks affecting the stability of the financial sector. There is also no existing security network that guarantees users' ability to recover their virtual assets in the event of loss or theft. Accordingly, the SCA addressed issues relating to consumer protection, safekeeping, technology governance, disclosure/transparency, market abuse and regulation of virtual asset platform use in a manner similar to the regulatory approach followed in relation to securities markets and commodity contracts globally.

13. The table below sets out the key risk areas, and the relevant mitigations for each of these risk areas, under the Virtual Assets Framework as follows:

Risks	Mitigation
AML/CFT \ Tax	Module Five of the Rulebook issued pursuant to the Chairman of the SCA's Board of Directors' Decision No. (13/Chairman) of 2021 on the Rulebook of the Financial Activities and Status Regularization Mechanisms related to anti-money laundering rules shall apply in full to all licensed bodies. Licensed bodies shall take into account any reporting obligations related to the Foreign Account Tax Compliance Act (FATCA) and the Common Reporting Standard (CRS).

Risks	Mitigation
Consumer protection	All material risks associated with virtual assets, accepted virtual assets and the products, services and activities of licensed bodies shall be appropriately disclosed, monitored and continuously updated.
Technology Governance	There shall be systems and controls regarding: • Virtual asset wallets (Digital Wallets). • Private Keys • Source and destination of virtual asset funds by applying the "Travel Rule". • Security procedures and measures, protection operations, systems testing and the ability to restore them. • Risk Management.
Virtual Asset Platform Activities	The Virtual Asset Platform Operator shall provide, among other things, the following: • Market monitoring. • Fair and orderly trading. • Settlement operations. • Recording transactions. • Rulebook . • Transparency and disclosure mechanisms. • Platform-like operational systems and controls.
Custody of Virtual Asset	Licensed bodies of virtual asset for safe custody activity, who provide safe custody and management services for acceptable virtual assets and enable control over them and/or client funds on behalf of clients, shall be subject to the safe custody provisions stipulated in Article 12 of Chapter Five of Module Three (Conduct of Business) of the Rulebook and the client funds provisions stipulated in Chapter Three of the same Module. Licensed bodies shall adhere to periodic review, compliance and reconciliation procedures and prepare reports on accepted virtual assets and client funds, in addition to appropriate internal controls to protect them.

Virtual assets activities subject to licensing and provision of financial services related to virtual assets:

14. Based on the Cabinet Resolution, the definition of virtual asset activities subject to licensing has come to reflect the definition issued by the Financial Action Task Force (FATF). The following activities shall subject to the SCA's licensing and control in accordance with the provisions of the Cabinet Resolution:
    - Providing services for operating and managing virtual asset platforms.
    - Providing exchange services between one or more forms of virtual assets.
    - Providing virtual asset transfer services.
    - Providing brokerage services in trading operations in virtual assets.
    - Providing services for safe custody and managing virtual assets and enabling control over them.
    - Providing financial services related to the issuer's offer and/or sale of virtual assets or participating in the provision of such services.

15. Based on the Cabinet Resolution, virtual assets activities were regulated in accordance with the Rulebook , and the Chairman of the SCA's Board of Directors' Decision No. (26/Chairman) of 2023 on the Regulation of the Virtual Asset Platform Operator, and as a result, the following licenses were made available:
    - Virtual asset platform operator.
    - Safe custody of virtual assets.
    - Financial consulting in virtual assets.
    - Managing portfolio of virtual assets.
    - Virtual Asset Broker.
    - Virtual Asset Dealer .

    It is worth noting that the virtual assets trading platform is considered equivalent in content to the Multilateral Trading Facility platform such as those used by counterparties.

Regulatory requirements for license applicants and licensed bodies for activities related to virtual assets

16. In order for the license applicant to be permitted to practice any virtual assets activities, the applicant shall satisfy the SCA that all applicable requirements of the SCA, including the relevant Rulebook , have been and will continue to be complied with. When the license applicant obtains the necessary license, he will have the same regulatory status as any other entity licensed by the SCA.

17. The basic rules and obligations for entities wishing to obtain a license to practice any virtual asset activities have been clarified within the Rulebook, which includes the following modules:
    - Module 1: General Provisions.
    - Module 2: Licensing and Accreditation.
    - Module 3: Conduct of Business.
    - Module 4: Capital Adequacy.
    - Module 5: AML/CFT

    In addition to the decision of the Chairman of the SCA's Board of Directors' Decision No. (26/Chairman) of 2023 on the Regulation of the Virtual Asset Platform Operator.

18. Module 1, (General Provisions), of Rulebook of the Financial Activities and Status Regularization Mechanisms shall apply to all licensed bodies. This module aims to provide the necessary guidance and controls for licensed bodies, with the aim of achieving maximum transparency and integrity in financial activities. The chapter specifies the standards and procedures that shall be followed to ensure flexibility and stability in the financial market, which reflects the continuous endeavor to improve the financial market environment.

19. Module 2, (Licensing and Accreditation.), of the Rulebook relating to licensing shall apply to all licensed bodies who practice any virtual asset activities, which requires compliance with all requirements stipulated in the aforementioned Module. This module constitutes a vital tool for achieving effective oversight of financial activities, which contributes significantly to enhancing the integrity and transparency of the market; as it is considered the

approved reference in determining the conditions and standards that must be provided to obtain a license to practice financial activities. In addition, the module stipulates the necessity of approving the employees working for licensed bodies, as it stresses the importance of having a qualified work team committed to ethical and professional standards. Licensed bodies and its employees shall commit to providing licensing and approval requirements on an ongoing basis in a way that enhances the integrity and stability of the market. Appendix No. 1 of module Two of the Rulebook also specifies the legal form and approved functions, in addition to the **capital requirements for each virtual asset activity as follows:**

- The virtual assets platform operator activity with a paid-up capital of (1) million dirhams in addition to maintaining an operating capital equivalent to the operating expenses for a period of (6) months if the virtual assets platform operator activity is carried out only without practicing any other activities related to virtual assets service providers, or (5) million dirhams, in addition to maintaining an operating capital equivalent to the operating expenses for a period of (6) months if the virtual assets platform operator is carried out, in addition to any of the other activities of virtual assets service providers.
- The activity of safe custody of virtual assets with a paid-up capital of (4) million dirhams, in addition to maintaining an operating capital equivalent to the operating expenses for a period of (6) months.
- Financial consulting activity in virtual assets with a paid-up capital of (500,000) dirhams.
- The activity of managing portfolio of virtual assets with a paid-up capital of (3) million dirhams.
- Virtual assets brokerage activity with a paid-up capital of (2) million dirhams.
- Virtual assets dealer activity with paid-up capital (30) million dirhams.

20. Operating expenses include all general and non-discretionary costs (variable and exceptional items can be excluded) incurred (or expected to be incurred) by the licensing SCA in its operations during a period of six months. Technology-related operational expenses, such as the use of IT servers and technology platforms, and the storage and use of IT equipment and technology services necessary for the overall operation of the virtual asset platform, can be included, with the possibility of excluding the development costs, such as research and registration of intellectual property patents.

21. Module 3 Conduct of Business shall apply to all licensed bodies who engage in a regulated activity in relation to virtual assets, which requires compliance with all requirements stipulated in the aforementioned module. Licensed bodies who operate a virtual asset platform or provide safe custody for virtual assets shall also comply with the additional requirements set out in Appendix 7 of the Rulebook relating to virtual asset wallets, to ensure appropriate activity is undertaken as part of their regulated activities. Module 3 forms an essential part of the Rulebook , with the aim of regulating the proper practice of the works of licensed bodies and specifying the obligations that they shall abide by while carrying out their work. This module includes a number of general obligations that all licensed bodies shall adhere to, in addition to obligations specific to each activity that has been licensed by the SCA. This module aims to enhance integrity and transparency in the securities and commodities market, and achieve a balance between effective regulation and encouraging innovation and sustainability.

22. Module 4 related to capital adequacy shall apply to all licensed bodies. Capital adequacy constitutes one of the basic pillars of ensuring the stability and safety of the financial market. This module aims to provide a strategic tool for monitoring the company with the aim of maintaining a safe level of capital to overcome financial challenges and maintain business continuity. As a regulatory body, the SCA aims, by setting requirements for capital adequacy, to protect the interests of investors by reducing the possibility of licensed companies defaulting, enhancing their ability to fulfill their obligations to clients, and instilling confidence in the safety of the virtual assets industry. The requirements also contribute to encouraging wise financial management, enabling companies to withstand economic fluctuations, adapt to market dynamics, and continue providing services to clients in a way that enhances the continuity of the virtual assets sector. Systemic risk management is a critical consideration in an interconnected financial landscape, as the capital adequacy requirements play a pivotal role in this regard by providing a safeguard against the domino effect resulting from failures in the virtual asset industry, preventing disruptions that could impact the broader financial ecosystem.

23. Module 5 for AML/CFT aims to provide a strong legal and regulatory framework to protect the market from the risks associated with money laundering and terrorist financing crimes, and to enhance the SCA's contribution to national and international efforts to combat these illicit phenomena. The Module also represents an essential part of the framework of controls and measures necessary to address serious financial crimes and to ensure the safety of the financial market and reduce potential risks. The module specifies the necessary procedures and policies that shall be taken by licensed bodies to reduce money laundering crimes and combat the financing of terrorism. It also specifies procedures for reporting and cooperating with the competent authorities to facilitate anti-money laundering and combating the financing of terrorism investigations. This module obligates licensed bodies to develop effective internal systems to detect and report any suspicious activities, which enhances effective cooperation to maintain the integrity of the financial system.

24. The Chairman of the SCA's Board of Directors' Decision No. (26/Chairman) of 2023 on the Regulation of the Virtual Asset Platform Operator applies to the virtual assets platform operator. This decision aims to establish the necessary controls and measures for the proper operation of the platform, which contributes to achieving stability and confidence in the virtual assets market. The decision includes a set of requirements that operators of virtual assets platforms shall adhere to, as this decision revolves around the SCA's desire to achieve a balance between encouraging technological development in the field of virtual assets and providing a safe and regulated operating environment. Appendix (1) to the decision also includes requirements for accepting the virtual asset within the platform operator's official list, which the platform operator shall apply to accept virtual assets for trading on the platform, with the aim of maintaining the quality of assets listed on the platform.

General Guidelines

Technology governance and controls

25. While the SCA takes a technology-neutral approach to licensing and regulating virtual asset service providers, virtual asset technology is widely considered to be in its early years of development and use. Although the SCA does not seek to regulate virtual asset technologies directly, it expects licensees to meet certain requirements in relation to their technology, governance and controls systems.

26. Historically, virtual assets business failures have often arisen as a result of insufficient technology-related procedures, including, for example, lack of security measures, systems development methodologies and limited system penetration testing to operate a robust business as well as the lack of technical leadership and management. Therefore, the SCA has developed specific guidance regarding expected controls and processes to help mitigate these issues.

27. Appendix No. 7 contained within module 3 of the Rulebook requires the licensed bodies, as a virtual asset services provider, to establish systems and controls to ensure that its affairs are managed effectively and responsibly, and to ensure that these systems and controls are subject to continuous monitoring and review, with a focus on:
    - Virtual asset wallets;
    - Private and public keys;
    - The source and destination of virtual asset funds;
    - Security;
    - Risk Management.
    - Protection operations and systems testing.
    - Encrypted keys and key storage.

28. When complying with Appendix 7 of Module 3 of the Rulebook , licensed bodies as virtual asset service providers shall consider the following key areas from a technology perspective:
    - Careful maintenance and development of systems and designs (e.g., control issuing the scripts, implementing updates, problem resolution, regular internal testing and third-party testing);
    - Security measures and procedures for safe storage and transmission of data;

- Business continuity and planning for client engagement in the event of planned and unplanned system outages;
- Processes and procedures that define personnel management and decision-making by qualified employees; and
- Procedures for establishing and managing services, interfaces and channels provided by or to third parties (such as recipients and providers of data or services).

Systems maintenance and development

29. Virtual asset service providers are expected to have a defined, documented and deliberate approach to implementing and updating systems and software.

30. Virtual Asset Service Providers shall also have well-established policies and procedures for regular and thorough testing of any system currently implemented or being considered for use (e.g., upgrading to a compatible engine or opening a new Application Programming Interface ("API") internally or with third party).

31. Virtual Asset Service Providers shall test the updated system for technical, operational and security vulnerabilities including, but not limited to, functional tests, penetration and stress tests. The test results shall be well structured, documented and signed by the responsible executives (technology specialists) of the virtual asset service providers.

32. All changes made to the script base used shall be tracked and recorded, with a clear audit trail for appropriate internal checks and sign-offs. Consideration shall be given to using an issuing control system that allows for precise timestamping and identification of the user responsible for relevant changes.

33. Virtual Asset Service Providers shall maintain a clear and comprehensive audit trail of internal system issues, including security and third-party issues, resolve them and implement fixes.

34. Virtual asset service providers shall conduct at least annual third-party verification/audit of the basic systems used (including, verification/audit of

custody arrangements and verification of the amount of their claimed holdings of virtual assets and client funds). The virtual asset platform operator and virtual asset custodians shall conduct an annual review of the infrastructure by reputable third-party cybersecurity consultants, producing a list of recommendations and areas of concern.

Security procedures and measures

35. Virtual asset service providers shall put in place measures and procedures that are consistent with best practices in network security (such as implementing firewalls, strong passwords, procedures related to password management, multifactor authentication, and encryption of data if it is stored or transferred).

36. All systems, especially security systems, shall be updated, and the gaps they suffer from shall be closed as soon as this can be done safely after issuing updates, whether the systems are developed internally or by a third party.

37. The IT infrastructures of virtual asset service providers (particularly in relation to multilateral trading facilities using virtual assets and custodians of those assets) are expected to provide robust, multi-layered security protection and seek to address "single points of vulnerability." Robust multi-level security policies for IT infrastructures shall be in place that specifically describe the robustness of multi-level security protections and how "single points of vulnerability" are addressed, including—but not limited to—the systems and procedures needed to restrict a particular user›s access to confidential client information.

38. IT infrastructure shall be robust enough to handle a number of scenarios without incurring significant losses to clients, including, but not limited to, accidental data destruction or breach, information leakage by current/former employees, or the successful hacking on a server or security unit of computer equipment, or enabling hackers to access a specific set of encryption/decryption keys, which may result in a complete breach of the system.

39. Virtual asset service providers shall establish information security policies and procedures for all employees. The security policy shall clarify the "security tone" throughout the entity and inform employees of what is expected of them. All employees shall be aware of the sensitivity of data and aware of

their responsibility to protect it. To mitigate "key persons risks", virtual asset service providers shall ensure that no particular person possesses confidential or sensitive information that is important to their operations.

40. Strong data encryption - both in storage and in transit - shall be included in the security policy. Specifically, strong cryptographic protocols and algorithms that are widely accepted by "cybersecurity" professionals shall be used to encrypt and decrypt the private keys of virtual assets. Important operations such as encryption, decryption, generating private keys, and using virtual signatures shall only be performed within encryption modules that comply with the highest applicable and internationally recognized security standards.

41. All security incidents and breaches shall be recorded and documented in the finest detail as soon as practically possible. Details regarding the solutions and steps to implement them shall be added to the record at a later date.

42. Open-source software shall be used in accordance with clear, transparent, and well-documented rules and procedures that regulate the stability, security, and suitability of the software for the purpose for which it is used. Any open-source software—whether compiled distribution or code— shall be accurately and thoroughly tested to identify operational and security vulnerabilities. The relevant executive officers of the Virtual Asset Service Providers shall agree to such testing before it is used to process or store operational and clients' data.

43. All internal and external APIs shall be secured by establishing strict access management systems and procedures, including encryption of information (such as SSL certificates). All activities related to accessing the programming interface shall be recorded and examined on an ongoing basis in order to detect any security breaches.

44. All changes to login credentials and access management procedures (for employees, third party service providers and clients) shall be subject to strict, well-documented procedures and rules. This shall include, but is not limited to, enforcing strong passwords, monitoring specific geographic locations via IP addresses, and using virtual private networks (VPNs), Tor program, or unencrypted links.

Cryptographic keys and wallets storage

45. The ability to send and receive virtual assets by adding a new transaction on a distributed ledger usually relies on encrypted keys - a public key and one or more private keys. The public key allows other users on the distributed ledger to send virtual assets to an address associated with that public key. The private key (or private keys) allows full control over the virtual assets linked to the public key. Accordingly, a virtual asset service provider shall take robust measures and strict security measures to ensure that the process of generating, storing, backing up and destroying public and private keys is secure both offline and in cases where they provide wallet services to their clients.

46. Whether private keys are held on network attached devices or devices that are offline, virtual asset service providers must have policies and procedures to ensure that they are not compromised by malicious actors.

Password protection and encryption

47. Virtual asset service providers shall consider the use of multi-signature wallets (i.e. those in which multiple private keys are linked to a particular public key and in which a subset of these private keys, sometimes held by different parties, must be used to authorize transactions). When 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).

48. Virtual asset service providers shall establish clear policies and procedures detailing recovery procedures when a client loses their login credentials. These policies and procedures shall cover the process of recovering private keys or regenerating lost private keys (e.g. using what is called a seed phrase, if possible).

49. Virtual asset service providers shall establish policies and procedures outlining the steps to be taken and responsibilities to be undertaken if private and public keys and client login credentials are compromised.

The source and destination of virtual asset funds

50. Transactions related to virtual assets take place between public addresses on a public distributed ledger. Although it is usually possible to determine the public addresses of the parties to a transaction, it is often very difficult to determine the identity of the owner of those addresses (whether a natural or legal person). This makes virtual assets attractive to money launderers, terrorist financiers and other criminals.

51. The US Office of Foreign Assets Control (OFAC) issued a statement requesting that wallet addresses known to be owned by individuals on the Specially Designated Nationals List ("SDN") and the Sanctions of Denied Persons List be reported. More information is available on the OFAC's[1] website. In addition, there are companies that collect "tainted" wallet addresses that have been used in hacks, "dark web" transactions, and other criminal activities

52. Virtual asset service providers shall establish policies and procedures that are consistent with their applicable anti-money laundering rules, with the aim of identifying the source of funds and ensuring their compliance with the guidelines established by the SCA related to anti-money laundering. These policies and procedures shall include due diligence measures related to withdrawals and deposits made by legal persons representing deposit holders or other multiple recipients of virtual assets. In connection with such deposits and withdrawals, Virtual Asset Service Providers shall have the ability to evaluate the wallet addresses of end beneficiaries and the sources or destination of their funds where appropriate.

53. It is important for a licensed person to conduct due diligence regarding his clients before opening an account in order to be able to identify users with wallet addresses. If a transaction originating from a "suspicious" wallet address belonging to a known user is detected, that user shall be reported. Virtual asset service providers shall maintain a list of "suspicious" wallet addresses and use third-party services to help identify such addresses if they do not have their own services to do so.

54. There are currently technical solutions developed internally and provided by third-party service providers; Through it, virtual assets can be tracked across multiple transactions to enable the source and destination of virtual assets to be determined more accurately. It is expected that virtual asset service providers will need to consider using such solutions and other systems to be able to fulfill their obligations related to anti-money laundering and combating financial crimes as well as those related to identifying clients in accordance with the framework for virtual assets.

[1] http://www.treasury.gov/resource-center/faqs/Sanctions/pages/faq_compliance.aspx

Planned and unplanned system outages

55. Virtual asset service providers shall have a planned system outage program to provide sufficient opportunities for updates and testing. Virtual asset service providers shall also have multiple communication channels to ensure their clients are informed in advance of any outage that may affect them.

56. Virtual asset service providers shall have clear and publicly available procedures outlining the process in the event of an unplanned outage. During the unplanned outage, authorized persons shall be able to disseminate key information and updates quickly and frequently.

Personnel management and decision making

57. Virtual asset service providers shall implement processes and procedures related to the decision-making process and access to sensitive information and security systems.

58. Clear audit records and review of the decision-making process shall be maintained. Employees who are responsible for decision-making shall possess sufficient experience - especially from a technical and professional perspective - that qualifies them for this.

59. Protection measures shall be implemented to limit access to sensitive/ important data to essential personnel only. This includes both digital and physical access. Virtual asset service providers shall develop processes and establish procedures to monitor and track access to all network resources. User login and logout mechanisms and the ability to track their activities are very important in preventing data breaches, detecting data breach attempts, or mitigating the resulting effects. Maintaining records facilitates accurate and comprehensive tracking, alerting and analysis in the event of any problems.

Outsourcing

With regard to the general requirements imposed by the SCA regarding outsourcing, it is necessary to adhere to what is stated in the Rulebook . The requirements below relate to the virtual assets wallet in particular:

60. Virtual asset providers may use services provided by third parties, but in doing so they shall assume absolute responsibility - from a regulatory standpoint - for any issues that may arise from the outsourcing of business and activities, including the failure of any third party to fulfill its obligations.

61. In its assessment of any potential third party service providers, a Virtual Asset Provider shall ensure that the service provider has developed robust processes and procedures in relation to the relevant service (including, for example, in relation to the testing processes and security measures set out in this module on technology governance).

62. In all circumstances in relation to outsourced business activities, virtual asset service providers are expected to have a strong understanding of the services provided by the third party and to have in place the necessary measures related to the underlying services where appropriate.

63. Public and private cloud service providers shall be subject to careful and comprehensive scrutiny. There shall be a specific and well-documented set of procedures related to access management. All service level agreements shall be reviewed annually to ensure their validity and ensure the security of the relevant systems and processes in line with the IT policies established by the virtual asset service providers. A "clear matrix of roles and responsibilities" shall be developed to define the service provider's operations and differentiate them from those of virtual asset service providers. Physical access to the systems shall be limited to relevant personnel. Virtual asset service providers shall monitor access by the authorized person on an ongoing basis.

64. Virtual asset service providers shall preserve data and be in a position to retrieve data stored in the cloud platform for the required period to achieve the SCA's record-keeping purposes. They shall also immediately provide the SCA with the data stored in the cloud platform in accordance with the directives issued in this regard.

65. Virtual asset service providers using cloud data storage services for the purpose of recording personal data shall comply with the rules of the regulatory SCA regarding data protection. It is also necessary to take into account the state from which the cloud storage provider operates or other arrangements that may facilitate compliance with applicable data protection regulations.

(Forks)

66 .Virtual asset service providers shall ensure that changes to the underlying protocol of the virtual asset that lead to forks are proactively managed and tested. This includes the temporary forks that shall be managed for backwards compatibility as long as it is required.

67. Virtual Asset Service Providers shall ensure that their clients are able to deposit and withdraw accepted Virtual Assets within and outside the Virtual Asset Service Provider's infrastructure on demand before and after the fork (except during live operation). Clients shall be notified in advance of any time periods during which deposits and withdrawals are not possible.

68. When the underlying protocol of a virtual asset (for example, the original token of that protocol) is changed, and the new version of that virtual asset is compatible with the old version (soft fork), the authorized persons shall ensure that the new versions and the old versions of the virtual asset continues to meet the relevant acceptable virtual asset requirements.

69. When the underlying protocol of the accepted virtual assets is changed, and the older version of the accepted virtual assets is no longer compatible with the new version and/or there is a completely new and separate version of the approved virtual assets (hard fork), the persons shall ensure that clients balances in the old version match with new version of virtual assets. Virtual Asset Service Providers shall also maintain transparent lines of communication with their clients on how the Virtual Asset Service Providers will manage clients› virtual asset holdings in such a scenario.

70. In the event of a hard fork, virtual asset service providers shall proactively manage any discrepancy between balances recorded in the previous version versus the new version by engaging with the community responsible for updating and supporting the underlying protocol for the relevant virtual assets. In addition, virtual asset service providers shall ensure that when they seek to provide services in relation to virtual assets associated with a new version of the underlying protocol, such new virtual assets meet acceptable virtual asset requirements and notify the SCA well in advance of offering the virtual assets, as part of their activities.

Protect client funds

71. Chapter Three of Module 3 of the Rulebook sets out the various requirements, to which the licensed bodies shall adhere in order to ensure that they protect client funds that they hold or control on behalf of their clients.

72. The bodies licensed for any virtual asset activities and that hold or control client funds shall adhere to the obligations specified in Clause Four of Article (3) of Chapter Three of Module 3 of the Rulebook . Licensed bodies are required to conduct audits and reconcile client funds, including but not limited to:
    - Conduct a daily review at the end of each business day of each client's accounting records to calculate his balance of cash amounts.
    - Settle client's accounts no later than the end of the business day following the day on which the reconciliation took place by covering the shortage of cash amounts or withdrawing any surplus during the same time period.
    - Notify the SCA if it is unable to reconcile or settle the accounts on the next day of discovering this.

Disclosure of risks of virtual assets

73. Given the significant risks to which clients dealing in virtual assets are exposed, virtual asset service providers are required to conduct detailed risk analysis and have processes in place that enable them to disclose, before entering into an initial transaction, all material risks to which their clients are directly exposed, in

a clear, fair and not misleading manner. As this disclosure obligation is ongoing, and given the rapid development of the virtual assets market, licensed bodies are required to continually update this analysis as well as the resulting disclosures to their clients to reflect any updated risks relating to:

- Products, services and activities of a virtual asset service provider;
- Virtual assets in general; and
- Selected accepted virtual assets.

74. The SCA expects that the disclosures that shall be made by a virtual asset service provider may include the following:
    - Virtual assets do not represent legal currency and are not backed by the government.
    - The values or process of valuing the virtual assets, including the risks of virtual assets having no value;
    - Volatility and unpredictability of virtual asset prices.
    - Trading in virtual assets may be subject to irrational market forces.
    - The nature of virtual assets may lead to an increased risk of financial crime;
    - The nature of virtual assets may lead to an increased risk of cyber-attacks;
    - The limited or, in some cases, no mechanism to recover lost or stolen Virtual Assets;
    - Risks of transacting virtual assets via new technologies (including distributed ledger technologies ("DLT")) relating to, among other things, anonymity, non-reversibility of transactions, incidental transactions, transaction recording and settlement;
    - The nature of Virtual Assets means that technological difficulties experienced by the licensed body may prevent access to or use of the client's Virtual Assets;
    - Any links to activities related to virtual assets outside the state, which may be unregulated or subject to limited regulation.
    - Any regulatory changes or actions by the regulating SCA or regulating SCA outside the state that may negatively impact the use, transfer, exchange and value of virtual assets.

Despite the disclosure of virtual assets risks above, the SCA believes that simply restating this non-exhaustive list of risks, whether in its application or in risk disclosure to its clients, may not be sufficient to include all of the risk disclosure requirements of a virtual asset service provider.

75. The introduction of a new accepted virtual asset for trading on the platform may require additional specific risk disclosure to platform clients in relation to the risks of trading in that new accepted virtual asset (as assessed by the platform).

76. Bodies licensed as virtual asset service providers shall clarify the mechanism by which the risks of trading in virtual assets will be disclosed to clients, in addition to any other relevant material risks. Disclosing these risks in the agreement to deal with the client may be the first opportunity for the licensed body to disclose this.

77. Given the increased inherent risks associated with investing in virtual assets and the SCA's goal of providing a regulatory system that provides adequate consumer protection, the SCA considers that all virtual asset service providers shall, before onboarding a client, ensure that the services, or new services proposed to be provided to the client, are appropriate, taking into account matters such as the relevant knowledge, experience and investment objectives of the client. Where a conflict is identified between inherent risks and suitability for the client, the licensed body shall take all reasonable steps to resolve this conflict.

Market abuse, transaction reporting and misleading impressions

78. The provisions on market misuse contained in Articles Nos. (17 ,16 ,15) of the SCA's Board of Directors Decision No. (2) of 2001 concerning the regulations as to trading, clearing, settlements, transfer of ownership and custody of securities also apply to market misuse with respect to virtual assets approved for trading on the platform.

79. The virtual assets platform operator shall report details of transactions in approved virtual assets traded on its platform. The SCA expects the Virtual Asset Platform Operator to submit reports to the SCA on a real-time and periodic basis.

80.In addition, the provisions contained in the SCA's legislation on misleading statements apply to approved virtual assets. The SCA expects that all communications (including advertising materials or other publications) by virtual asset service providers will be conducted in an appropriate manner and that a virtual asset service provider engaging in regulated activity in relation to virtual assets will implement appropriate policies and procedures to comply with the SCA›s requirements.

81. The SCA continues to consider developments in its regulatory structure in the context of the market abuse provisions, including for the purposes of any future determination as to whether the scope of the provisions shall be expanded to include virtual asset trading activity that is not specifically related to trading on the exchange. In this context, particularly in the case of virtual asset service providers such as the broker, the SCA reminds virtual asset service providers of their broader responsibilities under the Virtual Asset Framework in relation to the use of virtual assets, including in relation to client risk disclosure, suitability and best execution.

82. The SCA is aware that virtual asset platforms outside the state may not be subject to a regulatory standard similar to that applied by the SCA. Therefore, the SCA recommends that a virtual asset platform operator spend sufficient time considering the application of the Financial Crimes and Market Abuse Rule, what are the technology, systems and controls he proposes to use for these purposes, and the associated resource needed to adequately undertake these functions. For this reason, among other matters set out in these Guidelines, the SCA considers that it is not appropriate for a virtual asset platform operator to outsource compliance and market control functions to third parties.

Realistic requirements for virtual asset service providers

83 .In order to operate effectively as a virtual asset service provider, a licensed body carrying out regulated activity in relation to virtual assets shall commit resources of a nature that allow it to operate substantially in the state. Depending on the relevant regulated activities being undertaken, the SCA expects to see substantial resources committed inside the state across all lines of activity of a virtual asset service provider, including, but not limited to, commercial

activities, governance, compliance/control, operations, technology, IT, human resources and duties. The SCA expects that the cadres of the licensed body as a financial services provider will be present in the state.

Tax reporting

84. All licensed bodies shall comply with the implementation of the Foreign Account Tax Compliance Act (FATCA) and the Common Reporting Standard (CRS) including:
    - Cabinet Resolution No. (93) of 2021 implementing provisions of the Multilateral Administrative Agreement for the Automatic Exchange of Information and any amendments thereto.
    - Cabinet Resolution No. (63) of 2022 concerning the implementation of the Federal Decree No. (9) of 2016 ratifying the agreement between the government of the United Arab Emirates and the government of the United States of America to improve international tax compliance and to implement the Foreign Account Tax Compliance Act (FATCA) and any amendments thereto.
    - Chairman of the SCA's Board of Directors' Decision No. (21/ Chairman) of 2020 concerning the unified standards for tax reporting and any amendments thereto.

Appointment of consultants

85. The SCA advises the applicants for a license of virtual assets activities to consider appointing compliance consultants, as they have the appropriate skills, knowledge and experience (taking into account the activities that the applicant desires to undertake), to provide the required assistance to the applicant throughout the application process.

Applications for amendment or exemption

86. The SCA is aware that some rules, especially within the Rulebook , may not apply to some licensed bodies, and the SCA may grant an exception to the application of those Regulations to the extent that the license applicant or

licensed body believes that any other Regulations do not apply to it under its business model or etc. The SCA expects that the amendment or exception request will be submitted either as part of the license application or later time after the license is issued.

Obligations of licensed bodies to protect data for individuals

87. The Federal Law for the Protection of Personal Data (Federal Decree Law No. (45) of 2021 regarding the protection of personal data) constitutes an integrated framework to ensure the confidentiality of information and protect the privacy of community members by providing sound governance for data management and protection. The law sets general frameworks for dealing with individuals' personal data, how it is collected, processed and stored, as well as the means of ensuring its protection, and the rights and duties of all concerned parties. The law applies to the processing of personal data, whether in whole or in part, by means of electronic systems, inside or outside the state.

88. The law prohibits the processing of personal data without the consent of its owner, with the exception of some cases, including when processing is necessary to protect the public interest, or to establish any procedures for claiming rights and legal proceedings.

89. The law sets the following:

- Controls for processing personal data and the general obligations of companies that have personal data about individuals and those working in the field of processing personal data to secure the data and maintain its confidentiality and privacy, and the procedures and measures available thereto to ensure that it is not hacked, destroyed, changed, or tampered with.
- Controls on the cross-border transfer and sharing of personal data for processing purposes.
- Procedures for reporting a personal data breach. The law also grants the personal data owner several rights, including:
    1. Obtaining, free of charge, information and decisions made based on the processing of his personal data
    2. The right to request correction of incorrect or outdated personal data

3. The right to omission, which provides the individual with the right to request any company to which the law applies to completely delete his data.
4. The right to notification, which provides the consumer with the right to be notified if the system of a company to which the law applies is hacked, as he will be informed that his data has been breached.

90. Licensed bodies shall ensure that the personal data they process is:

- Processed fairly, lawfully and securely;
- B. Processed for specified, explicit and legitimate purposes in accordance with the rights of the data owner and is not processed in a manner that is incompatible with those purposes or rights;
- Adequate, relevant and not excessive in relation to the purposes for which it is collected or processed;
- Accurate, and updated as necessary; and
- Kept in a form permitting identification of data owners for no longer than is necessary for the purposes for which the personal data were collected or are being processed.

91. Licensed bodies shall, upon request, to provide individuals with access to any personal information they hold.

92. Licensed bodies shall keep records of all personal data processing operations that they carry out, and these entities shall immediately notify the SCA and the relevant authorities upon being aware of any security breach related to personal data.

93. Personal data may not be transferred and shared across borders except in accordance with the controls stipulated in the Federal Law for the Protection of Personal Data (Federal Decree Law No. (45) of 2021 regarding the Protection of Personal Data).

Transactions with unknown counterparties

94. Virtual Asset Service Providers shall avoid interacting transactions with any entity or service provider where the counterparty is unknown or anonymous (for example, via certain peer-to-peer exchanges or through a decentralized platform) at any stage of the process in and out of the core operations of virtual asset service providers. This is to ensure that virtual asset service providers remain compliant with the SCA's legislation at all times and do not unnecessarily expose their activities to risks arising from sources/destinations of tainted funds.

95. Virtual asset service providers shall also avoid including liquidity, pricing and settlement data from these entities in their daily operations. The SCA shall be notified immediately upon becoming aware of any interaction (whether intentional or not) with these entities.

Margin trading

96 .In the event of trading virtual assets on margin, the licensed body shall adhere to the margin trading rules issued by the virtual assets platform operator.

Insurance

97. The SCA recognizes the growing interest/interaction between virtual asset activities and the provision of insurance for these activities. Recognizing this, the SCA does not require licensed bodies to maintain insurance in relation to their virtual asset activities, as providing insurance is considered a second line of defense. As the first line of defense, the SCA expects all virtual asset service providers to ensure that their business operations are properly structured and to implement robust mechanisms to mitigate areas of actual and potential risk.

Specific requirements for each activity

Requirements of licensed bodies for virtual assets platform operator activity

98. A virtual asset may not be traded in the state unless it is accepted into the official list of virtual assets of the virtual assets platform operator licensed by the SCA and/or the competent SCA and the virtual asset is registered with the SCA.

99. The Virtual Assets Platform Operator shall undertake all tasks associated with the operation of the Virtual Assets Platform and the activities of the Virtual Assets Service Providers, and in this case, he shall comply with all the obligations of the Virtual Assets Service Providers specified in the Rulebook in addition to the obligations contained in the Chairman of the SCA's Board of Directors' Decision No. (26/)Chairman) of 2023 on the regulation of the virtual assets platform operator.

100. The virtual assets platform operator may simply operate the platform without engaging in any of the activities of other virtual assets service providers, and in this case, he shall comply with the obligations of the virtual assets platform operator mentioned in this decision.

101. The operator of the virtual assets platform shall register the virtual asset acceptable to him in the official list of the SCA before starting to trade it in accordance with the form prepared for that purpose by the SCA.

102. The virtual assets platform operator may collect the fees it deems appropriate related to virtual assets and the membership of its virtual asset service providers. The SCA has the right to monitor fees to ensure their proper application, and it may obligate the virtual assets platform operator to amend these fees in cases that so require.

Obligations of the Virtual Asset Platform Operator

Operational efficiency and flexibility

103. The virtual assets platform operator upon licensing and continuously after licensing shall comply with the following:

- Providing effective electronic programs and systems that are subject to regular review and development to monitor the trades and transactions that take place on the virtual assets platform.
- Maintaining the final record of ownership related to the virtual asset - where possible - via an electronic or digital network or (dematerialized) database, and refraining from issuing paper or written ownership certificates used for trading purposes.
- Providing flexible and powerful electronic programs and systems to ensure business continuity and disaster recovery commensurate with the nature, size and complexity of its operations, and to ensure continued fulfillment of its obligations and regulatory and legal requirements.
- Subjecting electronic systems and programs to stress tests and working to correct errors or weak points identified according to these tests as soon as they occur, and notifying the SCA of these tests and corrective measures if they are essential.
- Ensure that there are sufficient arrangements to conduct regular reviews of electronic systems and programs to ensure their continued adequacy and operation as intended.
- Providing internationally approved procedures to test the adequacy and effectiveness of its information technology systems.
- Taking appropriate measures to ensure the flexibility of information technology systems and they are not subject to failure; and a statement of its ability, in the event of failure, to continue working and protect information from damage, tampering, misuse, or unauthorized access, and from the integrity of data that forms part of information technology systems or is processed through them.

- Providing regular review and continuous updates to information technology systems and controls commensurate with the nature, size and complexity of the work by adopting well-defined development and testing methodologies that are clearly documented and consistent with internationally accepted testing standards.

- Providing a risk assessment and management system that specifies responsibilities for risk management, types of risks, the mechanism for measuring them, and how to treat them, including, but not limited to:
  1. Identify all general, operational and legal risks as well as the virtual asset platform operator risks wherever they appear in its activities.
  2. Measure and monitor different types of risks.
  3. Distributing responsibility for risk management to people with appropriate levels of knowledge and experience.
  4. Providing sufficient and reliable information to key individuals and the SCA.
  5. Monitoring and following up on transactions in its facilities.

- Providing appropriate procedures and arrangements to evaluate, test and monitor information technology systems on an ongoing basis as follows:
  1. Problem management and system change.
  2. Testing IT systems before live operations.
  3. Monitoring and reporting on the system performance and integrity.

Operational rules

104. The virtual assets platform operator shall, upon licensing and continuously after licensing, establish and maintain operational business rules in accordance with the following:
    - Rules and standards governing the acceptance of membership of its virtual asset service providers and any other persons provided with access to the virtual assets platform.
    - Rules and standards governing the acceptance of virtual assets.
    - Rules governing any failures or negligence in transactions.
    - Rules clarifying the mechanism for using the virtual assets platform for investors and prohibitions.

- Rules to ensure that the virtual assets platform complies with the Law on anti-money laundering and combating the financing of terrorism and the financing of illegal organizations and its executive regulations, and to track virtual assets to enable their application.
- Any other matters necessary for the proper operation of the Virtual Assets Platform.

105. The virtual assets platform operator shall, upon licensing and continuously after licensing, comply with meeting the operational rules of the following standards:
    - The operational rules shall be objective and not discretionary or biased.
    - The operational rules shall be clear and fair.
    - The operational rules shall specify the obligations of virtual asset service providers and other dealers as well as the other administrative arrangements when conducting transactions in its facilities or those related to the professional standards that shall be imposed on virtual asset service providers and/or dealers.
    - The operational rules shall be legally binding and enforceable on virtual asset service providers and other dealers.
    - The operational rules shall include provisions for resolving disputes between virtual asset service providers and other dealers and procedures for appealing decisions issued in their regard.
    - The operational rules shall include disciplinary procedures, including penalties.
    - The operational rules shall be available to the public free of charge.

106. The virtual assets platform operator shall provide adequate compliance procedures to ensure that operational rules are subject to monitoring and enforcement, and to promptly investigate any complaints related to its operations or related to virtual asset service providers and other dealers in its facilities, while taking disciplinary measures and referring cases to the SCA when necessary.

107. The virtual assets platform operator shall conduct a public opinion poll regarding its operational rules for a sufficient period and take into account the comments received from the public without prejudice to applicable legislations.

108. The virtual assets platform operator shall deposit the operational rules with the SCA after completing the public opinion poll.

109. The virtual assets platform operator shall make the necessary amendments and updates to the operational rules whenever necessary.

Integrity, transparency and professional behavior

110. The virtual assets platform operator shall provide a system that enhances and maintains high levels of integrity and transparency when conducting its business so that it enables all its clients to obtain the necessary information to understand the risks, fees, and costs associated with using its services and facilities.

111. The virtual assets platform operator shall ensure that the necessary measures are taken to:

- Record activities and transactions, including orders and audit records of orders made in or through its services and facilities.
- Maintain records of activity and transactions for at least 10 years.
- Protect applicable data and associated requirements.
- Refrain from using any information or procedures related to the virtual assets platform except to operate it and the virtual assets platform operator or its employees may not use this platform to make any private benefit.
- Refrain from disclosing user information or information related to anticipated listing operations for virtual assets to third parties other than for the purposes of the effective operation of the platform and the disclosures required in accordance with the SCA's decisions and applicable legislations.
- Immediately disclose information to the SCA and comply with its requirements from time to time, including suspending or canceling the trading of any virtual assets.
- Continuously disclose the high risks of investing in virtual assets to investors.

Protecting and preserving virtual assets

112. The virtual assets platform operator shall provide a system and procedures to separate its funds and virtual assets from the virtual assets and funds of clients and to separate the virtual assets and funds of each client from the other.

113. The virtual assets platform operator shall provide procedures for custody of and transferring virtual assets, recording account movements, identifying the registered client and beneficiary, and periodically reviewing and reconciling accounts.

Discipline and Commitment

114. The virtual assets platform operator shall provide an effective regulatory system, arrangements and compliance programs to monitor transactions and clients, prevent misuse and manipulations on the platform, and prevent misuse of the platform in contravention of applicable legislations regarding crimes of money laundering, combating the financing of terrorism and financing illegal organizations, and any other financial crimes. This is to ensure that the platform operates regularly, fairly and transparently.

115. The virtual assets platform operator shall provide the necessary measures to monitor the platform members' compliance with the applicable legislations in the State regarding anti-money laundering crimes, combating the financing of terrorism, and financing illegal organizations, and to ensure that they have appropriate arrangements and procedures to comply with those legislations.

116. The virtual assets platform operator shall notify the competent authorities and the SCA immediately upon learning of a violation of the applicable legislations regarding crimes of money laundering, combating the financing of terrorism, and financing illegal organizations.

117. The virtual assets platform operator shall provide policies, operational rules, and fair and objective procedures for accepting dealing in virtual assets, which include the following:

- Procedures for measuring the suitability of accepting a virtual asset on its official list in accordance with the requirements of Appendix (1) of the Chairman of the SCA's Board of Directors' Decision No. (26/)Chairman) of 2023 on the regulation of the virtual assets platform operator.

- Procedures for suspending and canceling the listing of virtual assets from the official list.
- Imposing obligations on any person to observe certain standards of behavior or to perform or refrain from performing specific acts.
- Identifying the actual or potential conflict of interest that arises or may arise when a person seeks to enter virtual assets on its official list.
- Any other matters necessary for proper operation.

Trading Regulation

118. The virtual assets platform operator shall establish rules and procedures for the fair, orderly and efficient operation of trading, provided that they meet the following:
    - Making relevant trading information available to investors to deal on a fair basis, including disclosing orders before and after the trading session.
    - Providing appropriate mechanisms to stop, suspend or cancel trading from its facilities for any virtual assets in circumstances where the requirements related to regulated trading are not met.
    - Providing controls to prevent fluctuations that do not result from the forces of supply and demand.
    - Providing controls and mechanisms to manage trading errors.
    - Providing short-selling controls, including lending and borrowing, monitoring short-selling and managing concentrations in positions.
    - Providing a fair and non-discretionary algorithm that matches orders.

119. The virtual assets platform operator shall provide adequate arrangements to continuously enhance transparency in the trading and post-trading phases by providing the trading public with sufficient information about the listed virtual assets as follows as a minimum:
    - Bid and ask price and quantity.
    - Price, volume, and degree of depth in announced prices and volumes, and time of transactions in real time and on a non-discretionary basis on electronic systems.
    - Any other information related to virtual asset operations that would enhance transparency.

120. The virtual assets platform operator shall provide effective systems, controls, procedures and arrangements to ensure the ability of trading systems to deal with trading fluctuations, including:
    - Sufficient flexibility and capacity when dealing with orders, volumes and messages at peak trading.
    - Work in an organized manner under stressful conditions on the virtual assets platform.
    - The possibility of rejecting orders that exceed the limits of pre-determined volumes and prices or that turn out to be clearly wrong.
    - The ability to cancel, change or correct any deal if necessary.
    - Preventing violations of capacity limits related to trading messages.
    - The possibility of requesting virtual asset service providers to apply pre-trading controls to their clients.

121. The virtual assets platform operator shall establish a comprehensive policy in the operating rules to address errors resulting from the entry of trading orders by mistake or resulting from a defect in the operating system, or both, provided that this policy clearly defines the extent to which orders and transactions can be canceled according to its absolute discretion or at the request of a member or with mutual consent of the relevant virtual asset service providers. In all cases, the virtual asset platform operator shall always:
    - Prevent or reduce wrongful transactions.
    - Identify and correct incorrect trades as soon as they occur.
    - Determine whether the erroneous transactions are related to unusual or inefficient trading.

122. Depending on whether a virtual asset platform operates a “member access” form or allows direct “client access», the SCA expects the virtual asset platform operator to have rules and a process for suspending or terminating access to its markets in circumstances where a client / member is unable to fulfill its obligations in relation to transactions related to accepted virtual assets.

123. The virtual assets platform operator shall provide arrangements, controls and procedures for settlement and clearing to ensure the fulfillment of the rights and obligations arising between the parties to the transaction executed on the platform, provided that it includes, at a minimum, informing the membership of its virtual asset service providers and other participants of those arrangements.

124. The virtual assets platform operator may present liquidity incentive programs for virtual assets on the platform under the following conditions:

- Limiting participation to platform members or to any other person for whom the virtual assets platform operator has taken due diligence measures to ensure that he has a good reputation, sufficient competencies and organizational arrangements, and has agreed in writing to comply with the rules of the virtual assets platform.
- Notifying the SCA in writing of the desire to present the program, provided that the notification includes the following:
  1. Program details.
  2. Benefits to the virtual assets platform, its members and other users.
  3. The start date of program implementation.

Organizing access to services

125. The virtual assets platform operator shall provide procedures that ensure access to its services and facilities only to permitted persons in accordance with legislations, operational rules and/or instructions, provided that these persons fulfill the following:

- Having a good enough reputation.
- Having a sufficient level of competence and experience, including appropriate standards of conduct for its employees who will be allowed to use the order entry system.

126. The virtual assets platform operator shall provide organizational arrangements, including financial and technological resources, that are no less than similar companies in the same field in accordance with global practices.

127. The virtual assets platform operator may allow virtual asset service providers to provide direct trading services to their clients according to the controls it sets and on the condition that they meet, as a minimum, the following:
    - Appropriate standards regarding risk controls and limits (Threshold) when entering through the direct trading service.
    - The ability to specify orders and transactions made through the direct trading service.
    - The ability to stop orders or transactions made by the client using the direct trading service without affecting other orders or transactions made or executed by virtual asset service providers.
    - The ability to assume responsibility for orders and transactions executed by clients who use direct electronic access.
    - Having sufficient mechanisms to prevent clients from submitting or executing orders using direct electronic access in a way that would lead any of the virtual asset service providers to exceed their margin limits or position.

128. The above-mentioned conditions do not apply to the virtual assets platform operator when it allows the investor to deal directly on its platform.

129. By not adopting a "member access" form and allowing "direct client access», virtual asset platforms lose a level of regulatory/supervisory defense that platforms or markets with member access enjoy, as they do not have members to assist them in conducting the necessary due diligence and compliance reviews of investors joining their markets. In such circumstances, the SCA requires virtual asset platforms operators to conduct its own due diligence reviews of every client accessing (trading) its markets (something a traditional member access trading platform or exchange could rely on its members to do). Hence, the resulting AML/CFT obligations fall directly on the platform operator.

Provision of the service of safe custody of virtual assets by the virtual assets platform operator

130. The virtual assets platform operator shall, in the event of provision of the service of safe custody of virtual assets, provide the appropriate separation between the responsibilities, employees, technology, and financial resources, as required, among the operations of the virtual assets platform and the safe custody of virtual assets.

131. The virtual assets platform operator may seek assistance of a third party custodian, but this shall not discharge it from its responsibilities towards its clients for custody of their virtual assets. Instead, the platform may by itself provide the safe custody services for the clients on their entire virtual assets as this shall be done internally without seeking assistance of any third party body that is licensed for safe custody. The virtual assets platform that provides the recommendation services in one of the above two forms, shall be deemed as providing safe custody for virtual assets for the purposes of regulation of virtual assets. The platform operator will be asked to comply with the provisions set out in Module 3 of the Rulebook , with compliance with the below stated guidelines concerning the safe custody of the virtual assets.

The accepted virtual assets

132. Article (3) of the Chairman of the SCA ›s Board of Directors› Decision No. (26/ Chairman) of 2023 on the Regulation of the Virtual Asset Platform Operator, allows the licensed body to practice a regulated activity only concerning the accepted virtual assets[2]. The licensed bodies such as a virtual assets platform operator shall have a general power for specifying every accepted virtual asset, provided that the virtual asset shall be registered with the SCA.

133. The virtual assets platform operator shall, upon filing a request for registering the virtual asset with the SCA, exert due diligence when evaluating and accepting the virtual asset in its official list by taking into account the guidelines set out in Annex No. (1) of the SCA ›s Board of Directors› Decision No. (26/Chairman) of 2023 on the Regulation of the Virtual Asset Platform Operator, that include:

[2]The Virtual assets platform operator shall submit a certificate, issued by a third party, confirmingits compliance with the guiding standards set out in Annex No.1 of the Authority's Board of Directors' Decision No.: (26/ Chirman) of 2023 on the Regulation of the Virtual Asset Platform Operator.

- Taking into account the situation and / or the regulations of the virtual asset that are applicable by the other regulatory authorities or the jurisdiction, and their appropriateness to the governance rules or arrangements therewith, whether the virtual asset is central or not; If the virtual asset is listed in the virtual assets green list or if it was accepted as appropriate for trading by a regulatory SCA or a jurisdiction; The historical record of the inspections carried out by the regulatory authorities concerning cyber security, combating money laundering, and the legal and regulatory rules related to the virtual asset; the existence of requirements by the regulatory SCA or jurisdiction where the virtual asset was created. In the event that the virtual asset is not central, the appropriate governance rules or arrangements shall be included in the principal protocol or the systems and rules applied for managing governance risks and conflict of interests.
- Taking into account the volume, liquidity and fluctuation of the virtual asset as clarified in the markets that are not regulated or that are internationally regulated, for example but not limited to: Taking into account the market efficiency degree and the term, period and date of the trading and transactions in the secondary market, the virtual assets services providers and the extent of presence of a record on the transactions volumes by their presence in the regulatory authorities or the jurisdiction; the total offered number of the issued virtual assets, the market value of the traded virtual assets, the predetermined time schedules for issuance or cancellation of the virtual assets, and the mechanisms of inflation or deflation; the factors affecting the supply and demand of the virtual asset and transparency concerning significant events affecting the price, the fluctuation levels and revenues; The virtual asset›s market liquidity, the daily and weekly trading volumes and the changes of liquidity level in response to the market pressures.
- To maintain transparency for technology, protocols, virtual assets holders and the parties associated with the virtual asset; for example: the information available for the public concerning developers, founders, miners, the main holders of virtual assets, and other principal persons who are associated with the virtual assets; the published white papers that clearly specify the purposes, uses and development path of the virtual asset, the history of previous initial offerings to the public and the uses of the money collected through those offerings; the ability of the public to have access the blockchain protocol, the compatibility mechanism, the open access to the records of live

updates on the blockchain, and publishing smart contracts and technology audit reports; the ability to keep the identification records concerning the virtual assets holders and the ability to track the virtual assets› balances and transactions and making sure of absence of the privacy preservation devices and the mix mechanism that may enhance concealing identity in the system.

- Ensure the efficiency and appropriateness of the technology; including: the blockchain type, authorization, the protocol amendment rights, the compatibility mechanisms and the environmental costs associated therewith; availability of smart contract, the self-calculation ability, the principal token advantages, and the ability to host the distinctive tokens on blockchain; the interoperability of several blockchains and the restrictions associated with the verification of transactions, time and costs; the technological solutions for collecting and protecting user privacy and controlling and maintaining user transaction records.

- The risks associated with using the virtual asset and the extent of the rules appropriateness to mitigate those risks including: the risks of anti-money laundering and the financing of terrorism, whether there is sufficient transparency concerning the virtual asset, whether there are suitable rules and regulations for dealing with money laundering, the financing of terrorism and the financial crimes risks in general; the cyber security risks and the rules of combating them, the date of hacks and thefts associated with the virtual assets, the imminent events and losses resulted from cyber security failure; the risks of preservation and the rules and regulations concerning the portfolio management, and the historical record of the user›s compensations resulted from the operational mistakes in the preservation management; the settlement risks, the mitigation measures, and the efficiencies and restrictions in achieving a final settlement when dealing with the virtual asset and using the external portals to reach the end; and The operational risks, the defense mechanisms, and the rules and regulations to prevent, detect and handle the wrong tokens, the quality assurance process and the risks interaction systems.

- In the event that the virtual asset has been previously registered with the SCA, the SCA will automatically accept the registered virtual asset.

Requirements of licensed bodies for the safe custody of virtual assets activity

134. The bodies licensed for the virtual assets safe custody activity («the virtual assets custodian») shall provide the service of assisting the clients to protect their accepted virtual assets. The virtual asset custodian term shall include the companies that only provide safe custody for virtual assets and clients› funds. However, the virtual assets platform operator may provide the virtual assets custody without obtaining an additional license.

135. In accordance with the approach followed concerning the activities carried out by the virtual assets' platforms, the SCA shall consider the activities carried out by the virtual assets' custodian as a main activity on the virtual assets. Accordingly, Module 3 (Business Practice) of the Rulebook includes additional specific requirements that apply to the bodies licensed for virtual assets safe custody.

Safe custody of clients› virtual assets

136. There are three general types of arrangements of safe custody of the virtual assets, that are likely to be adopted by the licensed bodies:

- **Type 1 (custodial wallet):** The licensed body 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 as the virtual assets' platform provides its 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 the virtual assets platforms, the virtual assets dealer, the brokers, and the portfolio manager) custodise their Accepted Virtual Assets. The virtual assets safe custody service provider of the type (1) shall efficiently keep the virtual assets (for example, the private keys) as agents acting on behalf of the clients and it shall control those accepted virtual assets. (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.)

- **Type 2 (Outsourced custodial wallet):** The body licensed for the virtual assets safe custody activity may seek assistance of external entities for performing the operational aspect of this function by outsourcing to a third party for practicing the activity of virtual assets safe custody. However, the licensed body shall remain bound to bear full responsibility for the safe custody of the clients› accepted virtual assets. The arrangements of this scenario shall also include the outsourcing of the virtual assets safe custody services by the virtual assets platform operator to a third party who is licensed as a virtual assets safe custody service provider, but the platform operator shall remain responsible at all times towards the clients for protecting their accepted virtual assets.
- **Type 3 (Non-Custodial wallet / Self-custody wallet):** Under this scenario, the licensed body allows/requires Clients to wholly "self-custodise" their Accepted Virtual Assets, and at no point does the licensed body 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' authorization.

137. The entities providing the services of virtual assets safe custody according to scenarios 1 or 2 above, shall be generally deemed as a provider of the virtual assets safe custody services and they should obtain the required license from the SCA.

138. 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 for the provider of the virtual asset safe custody. The SCA 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. Furthermore, the licensed bodies who request from the clients to provide self-custody for the virtual assets should fully and clearly reveal this fact to the clients in advance and it should meet the disclosure standards set out in this guidelines. The SCA will take into account the quality of these suggested disclosures when evaluating the requests filed by the licensed bodies who suggest requesting from the clients to provide self-custody for their virtual assets.

139. A licensed body that keeps or controls the accepted virtual assets, on behalf of its clients, shall meet all the obligations of the virtual assets custodian mentioned in Module 3 of the Rulebook .

140. In this regard, the virtual assets platform operator who provides an integrated virtual assets wallet, shall comply with the safe custody rules set out in Module 3 of the Rulebook . Moreover, the virtual assets platform operator shall, in the event of outsourcing its virtual assets wallets to a third party, comply with or ensure the compliance with the rules of virtual assets safe custody, as required.

Obligations of brokers / dealer of virtual asset

141. The virtual assets services providers who intend to work only as brokers or dealer for the clients (including the running of brokerage offices or the dealing outside the stock exchange) shall not be allowed to regulate the service or the brokerage / their trading platform in a way that may be deemed as running a market or a virtual assets platform. The SCA shall consider advantages such as allowing the prices discovery, displaying the general trading orders book (it is accessible for any individual of the public, regardless of whether they are clients or not), allowing to perform automatic matching of transactions using a matching engine according to the stock exchange type, of the virtual assets platform features, not the activities that the virtual assets services provider of the broker type can perform.

142. The body that is licensed as a virtual assets services provider whose license is limited to provision of financial services for working as a broker / dealer not as an operator of a virtual assets operator, should design and regulate its operations, the user interface, the website, the marketing materials, and any public thing, or the information directed to the client, so that the same shall

not create an impression that he operates a virtual asset platform. Practically, this may include the display of any generally accessible information that may seem as a trading book, along with non-provision of any price discovery and not giving impression to the actual or potential clients that they are interacting with a virtual assets platform.

143. The brokers / the virtual assets dealers shall comply with the execution price best requirements set out in Chapter 4 / Article 7 of the Module of Business Practice, at all times.

144. Keeping the data related to the date, time, purchase and sale price, and number and type of the virtual asset subject of the trading transactions and the disclosures related thereto.

Obligations of the financial consulting company in virtual assets

145. The financial consulting company in virtual assets shall set appropriate procedures and rules for ensuring that the financial consulting issued for the client is valid and neutral and includes the required disclosures, along with documenting and archiving all those disclosures and everything submitted to the client or of which the client is notified.

146. The financial consulting company in virtual assets shall comply with the following when preparing and publishing the analysis report, the financial planning, or the financial recommendation:

- Specifying the names and addresses of the persons who participated in preparing the report.
- Specifying the date of the report preparation and the covered period.
- Specifying the relation between the licensed body and all the authorities relevant to the report.
- Specifying that the recommendation included in the report is a technical opinion without ensuring the results.
- Avoiding exaggerated words, promises, impressive words, cheating, fraud, misleading, or manipulation of emotions.
- Using terms like expectations predictions, estimations, or assumptions in preparing the report.

- Using the words (purchase), (sale), or (keeping) in the financial recommendation report.
- Specifying the mechanism used for estimation and evaluation and the relied upon assumptions and comparisons.
- Specifying the source of the relied upon information and data.
- Specifying the types of the mainly targeted clients.
- Preparing a table or a diagram showing the targeted prices included in the previous analysis reports - for one previous year at least if any - for the same financial product and / or virtual asset subject of the analysis report compared with the actual prices on the date expected for achieving the targeted prices as mentioned in those reports.
- Distinguishing between facts and opinions or estimations.
- Taking the required steps for enabling the client to recognize the nature of the risks associated with implementation of the recommendations associated with the financial recommendation report.
- Stating clearly that the normal investor should not rely on the report in the event that the financial recommendation is designated for professional investors or the corresponding party only.
- The report should be approved by the senior management or its authorized representative.

Disclosure to the client

147. The financial consulting company in virtual assets shall disclose any financial or material interest of the licensed body, the financial analyzer or his spouse or minor children, as for the virtual assets, subject of the financial consulting.

148. The financial consulting company in virtual assets shall disclose any relation between the licensed body, the financial analyzer or his spouse or minor children, and the issuer of the virtual asset, subject of the financial consulting, or the fact that it received any consideration from it.

149. The financial consulting company in virtual assets shall disclose the properties owned by the licensed body or any of its financial group of a percentage of

(%1) or more than this, or the properties owned by the financial analyzer or his spouse or minor children, in the issuer of the virtual asset, subject of the financial consulting.

150. The financial consulting company in virtual assets shall disclose any arrangements or rewards that may represent a conflict of interest and that are likely to fully or partially affect or reduce the quality of the financial consulting.

151. The financial consulting company in virtual assets shall disclose any services provided to the issuer of the virtual asset, subject of the financial consulting, within (12) twelve days before providing the consulting or any services expected to be provided to the issuer of the financial product within (3) three months after provision of the financial consulting.

152. The company of financial consulting in virtual assets shall disclose any material contribution by the virtual asset issuer in the licensed body.

Prohibitions for a financial consulting company in virtual assets and its financial analysts

153. The financial consulting company in virtual assets and its financial analysts are prohibited from owning the virtual asset that is the subject of the financial consultation or any of the financial derivatives associated with it during the cooling off period.

154. The financial consulting company in virtual assets and its financial analysts are prohibited from trading in the virtual asset that is the subject of the financial consultation or trading in any of the financial derivatives associated with it during a period of fifteen (15) days before issuing the financial consultation and a period of five (5) days after issuing the financial consultation or issuing any accompanying financial consultation includes an amendment or change in the recommendation or target price, unless it was owned before starting the financial consultation.

155. The financial consulting company in virtual assets and its financial analysts are prohibited from trading in the virtual asset that is the subject of the financial consultation or from trading in any of the financial derivatives

associated with it in a manner that violates the recommendations contained in the financial consultation for a period of no less than (30) thirty days from the date of issuance of the financial consultation report.

156. The financial consulting company in virtual assets and its financial analysts are prohibited from publishing or submitting any report associated with to the virtual asset if it is a main financial advisor or participant with the issuer of the virtual asset.

157. The financial consulting company in virtual assets and its financial analysts are prohibited from providing or publishing financial consultation or disclosing or declaring it by any regular or electronic means about any virtual asset if it or any of its board members, manager, financial analysts or employees receive material or moral compensation, (directly or indirectly), whatever its form or type, from the issuer of the virtual asset or any party related to it.

158. The financial consulting company in virtual assets and its financial analysts are prohibited from including in the report any incorrect or misleading information or data.

159. The financial consulting company in virtual assets and its financial analysts are prohibited from providing advice to a client that contradicts or conflicts with the recommendations of the report issued by it, unless it discloses the reasons for this conflict before providing advice to the client.

160. The financial consulting company in virtual assets and its financial analysts are prohibited from exerting any type of material or moral pressure (directly or indirectly) on the financial analyst while performing his work duties to influence his neutral technical opinion regarding the issuer of the virtual asset that is the subject of financial consultation.

161. The financial consulting company in virtual assets and its financial analysts are prohibited from giving specific prices for a specific financial product if the company is under establishment.

162. The financial consulting company in virtual assets and its financial analysts are prohibited from agreeing with the issuer of the virtual asset or any other parties with the intention of causing an impact on the prices of its products or its financial position other than the truth.

163. The prohibition contained in Clauses (159 ,158 ,157) applies to everyone who contributed to the preparation, review, or approval of the financial consultation, their spouses and relatives up to the first degree, and everyone who is aware of the content of the financial consultation from members of the Board of Directors and the executive management of the licensed company and its managers and employees and their relatives up to the first degree. The prohibition does not apply in the following cases:
    - If the ownership takes place before starting the financial consultation.
    - B- If a fundamental and unexpected change occurs to the financial position of any of the persons subject to prohibition, after obtaining written approval from the compliance officer.
    - If any of the persons subject to prohibition has contributed to an investment fund that trades in the financial product that is the subject of the financial consultation, provided that the ownership percentage of any of them does not exceed (%1) of the total assets of this fund and that the percentage of this fund's investments in this financial product does not exceed a total of (%20) of the fund's assets.
    - If important events or material information occur which lead to changing the subject of the financial consultation, after obtaining written approval from the compliance officer.

Obligations of portfolio management activities for virtual assets

164. The portfolio management activities for virtual assets shall:
    - Achieve the client investment goals agreed upon with him.
    - Form an investment committee by decision of the company's board of directors, which is responsible for planning the implementation of the investment policy for investment management, follow up and monitoring actual performance, and control it and periodically review the rules and procedures necessary to practice the activity at least twice a year.
    - Manage the investment wallets of its clients according to an agreement with them based on the discretion of the wallets manager without the client's intervention (Discretionary) or based on a decision taken by the client himself (Non-Discretionary).

- Disclose to the client data and information related to the evaluation of his investment in a manner consistent with the client classification and its investment objectives.
- Take into account the provision of an amount of liquidity commensurate with the nature of the investment that he is responsible for managing to confront the risks and obligations associated therewith.
- Provide the client with a monthly statement of account, unless the agreement concluded between them stipulates a shorter period, provided that the statement of account includes, as a minimum, the data contained in Appendix No. (3) of Module 3 (Conduct of Business) of the Rulebook.
- Exert everything it can to study the virtual assets in which the client's funds that you manage are invested, and diversify such investments to reduce the investment risks to which it may be exposed, in accordance with the investment policy, and not use such funds to influence the prices of virtual assets on the platform.
- Receive orders from clients in accordance with the procedures stated in (First) of Article (1) of Chapter 5 of the Rulebook if the wallets management is based on the clients' decisions (Non-Discretionary).
- Refrain from executing margin trading orders in the clients' pooled account.
- When executing his clients' orders based on the clients' decisions (Non-Discretionary), execute the trading order in accordance with the trading order issued by the client, and that the execution be in a timely manner immediately after the order is issued by the client, and to execute the trading orders for the private wallets management company's accounts – in case of obtaining approval of the same from the market or the SCA, as the case may be, and trading orders for its client's in a fair manner and in accordance with the priority and precedence of their receipt.
- Refrain from executing excessive trading orders, and refrain from exploiting clients' data, transactions, and trading orders to achieve benefits or gains for the broker, its employees, or others, and maintain their confidentiality.
- Notify the client of the trades that took place in its account in accordance with the procedures contained in (Fourth) of Article (1) of Chapter 5 of the Rulebook .

An overview of anti-money laundering (AML), combating the financing of terrorism (CFT) and sanctions evasion

165. The use of virtual assets is a topic which raises numerous regulatory concerns for regulators, supervisors and law enforcement agencies around the world, especially in relation to money laundering (ML), terrorist financing (TF) or evasion of targeted financial sanctions. International bodies and organizations such as the International Monetary Fund (IMF), Financial Action Task Force (FATF), Bank for International Settlements (BIS), and the International Organization of Securities Commissions (IOSCO) have issued multiple warnings regarding virtual assets. These warnings are intended to inform investors and market participants of the high risks associated therewith, including the risks of money laundering, terrorist financing, and other financial crimes, as well as the potential of exploiting virtual assets for illegal activities on a large scale. "This global challenge affirms the urgent need to develop effective and balanced legislative, regulatory and supervisory frameworks that ensure security, financial stability and integrity without compromising innovation and development in the field of digital assets."

166. The Financial Action Task Force (FATF) has identified some of the key risks associated with virtual assets[3], which include the following:

- **Virtual Assets and Privacy:** Virtual assets in particular may operate in a way which provides a high degree of privacy; as its trading takes place through website platforms, it is usually characterized by indirect relationships with clients, allowing for anonymous financial transfers, whether through cash financing or financing from a third party through "virtual exchanges," which may fail to identify the exact source or destination of the money.
- **Cross-border risks:** The global spread of virtual assets increases the risks of money laundering and terrorist financing. These assets are available online, including via mobile phones, facilitating their use for cross-border payments and money transfers.

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

- **Infrastructure complexity:** Virtual asset platforms rely on complex infrastructures which involve multiple entities, often extending to multiple countries. This leads to a lack of clarity in responsibilities regarding compliance with anti-money laundering and combating the financing of terrorism legislation. It is also difficult for regulators and law enforcement agencies to access client and transaction records distributed in different countries.
- **Weak internal controls:** Some components of the virtual assets system or its service providers may be located in countries that lack adequate controls to combat money laundering and terrorist financing crimes.
- **Market Manipulation:** Virtual assets are vulnerable to market manipulation due to weak regulatory oversight, resulting in sharp price fluctuations and increasing risks to investors.
- **Vulnerability to cyber-attacks:** Due to their reliance on technology, virtual assets and the platforms that trade them are more vulnerable to cyber-attacks, threatening the security and privacy of assets and personal data.
- **Technological challenges:** Rapid technological developments in the field of virtual assets, including the use of blockchain technologies and smart contracts, pose additional challenges in terms of tracking and control. This diversity of uses of these technologies increases the difficulty of developing effective regulatory and controlling frameworks.

167. On 22 February 2019, the Financial Action Task Force (FATF) acknowledged the importance of addressing the money laundering and terrorist financing risks associated with digital assets through a public statement. This acknowledgment came as a response to the rapid developments and emerging challenges in the digital assets market. According to this statement, the Financial Action Task Force proposed additional details on how to regulate and control virtual assets (VAs) and virtual asset service providers (VASPs). These details were provided in the draft Explanatory Note to Recommendation No. 15 dealing with "new technologies". This Note aims to provide a clear and specific framework for dealing with financial risks related to digital assets and enhancing supervision and control over them. Through these steps, the Financial Action Task Force sought to achieve a balance

between promoting innovation in the field of digital assets and ensuring financial security and stability and the market's compliance to standards of transparency and combating money laundering and terrorist financing.

168. On 21 June 2019, the Financial Action Task Force issued guidance on the risk-based approach (RBA) for virtual asset service providers, as well as an explanatory note to Recommendation No. 15. This guidance was based on previous statements provided by the Financial Action Task Force to clarify the risk-based approach (RBA) in the field of anti-money laundering and combating the financing of terrorism (AML/CFT). The basic principle, on which Guidance of Financial Action Task Force is focused, is that asset service providers are expected to "identify, assess and take effective measures to mitigate money laundering and terrorist financing risks" in relation to virtual asset services.

169. Furthermore, the purpose and scope of the Financial Action Task Force Guidance is to clarify and assist:

- Regulatory authorities in the State: The guidance helps regulatory authorities understand and develop regulatory and supervisory responses to virtual asset activities and their service providers, with a focus on applying a risk-based approach. This includes developing flexible legislative and regulatory frameworks that are compatible with technological advances and market challenges.
- Countering Money Laundering and Combating the Financing of Terrorism: Directing supervision and control of asset service providers and service providers to ensure compliance with international standards in the field of countering money laundering and combating the financing of terrorism. Affirming the need to develop an effective compliance program and internal controls, including employee training to identify suspicious activity.
- Licensing and registering virtual asset service providers: Providing guidelines for licensing or registering virtual asset service providers based on applicable requirements, taking into account the importance of effective systems for controlling and supervising countering money laundering and terrorist financing crimes.

- Developing internal controls and preventive measures: Enhancing the importance of building a compliance program to counter money laundering crimes and combat the financing of terrorism through developing internal controls and preventive measures such as client due diligence, record keeping, and reporting suspicious transactions. This includes using advanced techniques to analyze data and detect suspicious patterns.
- Sanctions and international cooperation: The importance of executing sanctions and other enforcement measures, in addition to international cooperation in this context and strengthening international mechanisms for exchanging information and cooperation between countries.
- Understanding Risk Indicators: Specific guidance for understanding risk indicators related to virtual assets, especially regarding suspicious transactions or restrictions affecting the ability of virtual asset service providers to identify clients.

170. The main explanatory notes to Recommendation (15) include the following:

- Virtual assets are considered "property", "proceeds", "money", "money or other assets" or other "corresponding value", which requires the application of internal controls and measures to mitigate the risks of money laundering or other related crimes under the Financial Action Task Force Recommendations on virtual assets and their service providers.
- Recommendations 10 to 21 are proposed to apply directly to virtual asset service providers taking into account the following:
    1. Under Recommendation No. 10 of the Financial Action Task Force, specifically designed for virtual asset service providers, special importance shall be given to applying enhanced due diligence (EDD) procedures to large transactions. Specifically, virtual asset service providers are required to adopt enhanced due diligence procedures for any transaction whose value exceeds (USD 1,000 - AED 3,500 depending on the legislation in force in the State). This procedure includes an in-depth and comprehensive examination of transactions to identify and reduce high risks related to money laundering and financing of terrorism. Enhanced due diligence procedures include

detailed checks to determine the identity of the client, the nature of the transaction, the source of funds, and the purpose of the transaction. This approach ensures that virtual asset service providers remain alert and proactive to identify and confront any potential risks associated with large transactions, which contributes to maintaining compliance with international standards and legislation in force in the State, which contributes to ensuring the integrity of the financial system.

2. Recommendation No. 16 issued by Financial Action Task Force provides basic guidance to virtual asset service providers regarding the implementation of the "Travel Rule". This rule requires that basic information (transfer originator - sender) and beneficiary in virtual asset transactions are obtained, maintained, and provided when necessary. The goal of the "Travel Rule" is to enhance the transparency and traceability of virtual asset transactions, which contributes to the identification and reporting of suspicious activities, in addition to enabling the implementation of funds freeze measures and blocking of transactions related to specific persons or entities. To ensure compliance with Recommendation 16, virtual asset service providers must establish effective systems, procedures and internal controls. This includes obtaining and securely storing client information, especially those related to information of (originator of the sent transfer) and beneficiary in the transactions. Furthermore, it is necessary that virtual asset service providers have mechanisms in place to quickly and efficiently provide this information to the relevant authorities upon request.

3. Virtual asset service providers must develop and implement a compliance program to counter money laundering, combat financing of terrorism, and apply the targeted financial sanctions, including robust policies, procedures, and controls that clarify how to gather, store, and transmit the required information in accordance with the standards of the Travel Rule. It is also important to conduct periodic evaluations to examine the effectiveness of these procedures and make the necessary improvements to maintain an ongoing high level of compliance.

171. To develop an effective and sustainable regulatory framework for virtual assets, the SCA considers full compliance with the framework to combat money laundering and terrorist financing an essential matter. This includes, but is not limited to:
    - Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering crimes and Countering the financing of terrorism and illegal organizations, and its amendments.
    - Cabinet Resolution No. (10) of 2019 on the executive regulations of Federal Decree-Law No. (20) of 2018 on Anti-Money Laundering crimes and Countering the financing of terrorism and illegal organizations, and its amendments,
    - Cabinet Resolution No. (74) of 2020 concerning the UAE list of terrorists and implementation of UN Security Council decisions relating to preventing and countering financing terrorism and leveraging non-proliferation of weapons of mass destruction, and the relevant resolutions.
    - Cabinet Resolution No. (109) of 2023 on Regulating the Beneficial Owner Procedures
    - Cabinet Resolution No. (111) of 2022 Concerning the Regulation of Virtual Assets and their Service Providers..
    - Module 5 of the Rulebook for Financial Activities: Controls on Anti-Money Laundering crimes and combating the financing of terrorism and the financing of illegal organizations.
    - The joint guide issued by the UAE Supervisor Authorities regarding countering money laundering crimes and combating the financing of terrorism for financial institutions.
    - Guidance on targeted financial sanctions: for financial institutions, designated non-financial businesses and professions, and virtual asset service providers.

172. In addition to the above, taking into account the risks associated with money laundering and terrorist financing in the virtual assets sector, the SCA expects virtual asset service providers to adopt international best practices (including FATF recommendations and including adherence to standards and specific guidance to counter money laundering and financing of terrorism crimes, and apply the necessary procedures to build an integrated compliance system and effective internal controls to verify the identity of clients and control suspicious financial activities...etc.

Key considerations when complying with AML/CFT

173. When considering the FATF's recommendations, applying the rules of AML/CFT and evading the application of targeted financial sanctions, the Securities and Commodities SCA clarifies that licensed bodies who conduct regulated activity in relation to virtual assets must take into account the following basic principles:

First Principle: Responsibilities

174. This principle requires virtual asset service providers to fully understand and fulfill their responsibilities with regard to the legislation regulating AML/CFT. This includes a commitment to building an integrated compliance program and implementing the necessary procedures to study business risks and client risks to which virtual asset service providers are exposed, verify the identity of clients, monitor and report suspicious financial activities in accordance with international and local standards. It also requires service providers to ensure that their employees are adequately trained and develop effective internal control and risk management procedures to deal with challenges related to Money Laundering and the Financing of Terrorism in the nature of the activity and services provided thereby.

Second Principle: Risk-Based Approach

175. The FATF expects countries, supervisory and regulatory authorities, financial institutions and other interested parties to adopt a "risk-based approach" (RBA). Licensed bodies must understand the risks associated with their activities and allocate appropriate resources to mitigate these risks, enabling them to make decisions and allocate resources efficiently and effectively.

176. Licensed bodies must conduct regular and appropriate assessments of the risks of their business and activities. In order to implement the risk-based approach effectively, they are expected to have specific processes in place to identify, assess, monitor and manage and mitigate the risks of money laundering, terrorist financing and targeted financial sanctions evasion. Internal controls and enhanced risk management and mitigation measures must be in place and effective in situations where money laundering risks are higher.

177. Identifying and understanding the impact that a licensed body (such as a virtual asset service provider) can have on its business relationships with correspondent foreign financial institutions represents an important challenge. This also involves assessing how financial institutions are perceived by regulators in the light of these emerging relationships. A key element in this context is the effectiveness of financial institutions› compliance programs, including their ability to continuously monitor the activities of the licensed body.

178. Correspondent foreign financial institutions (including virtual asset service providers) rely heavily on the strength and efficiency of compliance programs implemented by local financial institutions. They assess the extent to which such programs can detect and prevent attempts at money-laundering and terrorist financing. Therefore, establishing a robust and comprehensive compliance program, which includes ongoing and effective monitoring of financial activities, is vital to maintaining successful and sustainable business relationships with correspondent foreign financial institutions.

179. With the increasing use of encryption and blockchain technologies in financial services, financial institutions that provide financial services to person/body licensed to practice the activity of virtual asset service providers must ensure that this licensed person/body is well organized and has appropriate systems and controls to address the risks of money laundering, terrorist financing and applying targeted financial penalties. These systems and controls must include robust due diligence processes for clients and beneficiary owners, transaction control, and the readiness and ability of the licensed person/body to provide full transparency to its financial institutions and the correspondent foreign financial institution when necessary.

Third Principle: Business Risk Assessment

180. The people concerned are requested to take appropriate steps to identify and assess the risks of money-laundering facing their businesses, taking into account their nature, size and complexity. This also requires considering the use of new technologies. In particular, in the context of virtual assets, FATF Recommendation No. (15) stresses the need to assess risks before launching new products, new business practices, or using new or advanced technologies, while emphasizing on taking appropriate measures to manage and mitigate those risks.

181. Understanding the virtual assets industry: Licensed bodies, their management and employees shall familiarize themselves with the characteristics and terminology related to the virtual assets industry. Furthermore, they must be aware of the potential for virtual assets to be misused in criminal activities and understand the technical and complex nature of these assets and the platforms on which they operate.

182. Comprehensive risk assessment: When conducting a risk assessment, a licensed body shall consider all aspects of business risks. For example, issues related to cybersecurity, such as transactions with hot wallets or the use of cloud computing to store data, should be viewed as technological risks that can also impact Money Laundering and the Financing of Terrorism risks, technology governance and consumer protection. The licensed body shall use the assessment results to develop and maintain an effective compliance program to counter money laundering crimes.

Fourth Principle: Client Risk Assessment and Client Due Diligence

183. Client Assessment: The SCA expects virtual asset service providers to carry out client risk assessments that are fully compliant with applicable legislation. Due to the anonymity features of virtual assets, tracking client records and transactions becomes a major challenge for compliance officers.

184. Due Diligence Policies and Procedures: All virtual asset service providers shall implement "client due diligence" policies and procedures. This includes assessing and evaluating all clients according to their risk profile, and this assessment shall be done before transacting any business on behalf of the client.

185. Indirect dealing and verification of the client's identity: In the case of indirect dealing, licensed bodies shall establish appropriate policies to ensure accurate verification of the client's identity.

186. Use of new technology: Licensed bodies can use new technology such as facial recognition programs and other biometric technologies, especially those issued by government agencies in the state, to improve risk assessment processes and verify clients' documents.

187. Verification and risk mitigation techniques: The Securities and Commodities SCA recognizes the importance of using technologies such as fingerprints, retinal scanning, and the use of video technologies to improve the process of verifying a client's identity and mitigate the risks associated with the use of virtual assets.
188. Collection of additional information: The Securities and Commodities SCA recommends that virtual asset service providers obtain additional information to assist them in the assessment and verification process in accordance with the SCA's Board of Directors Resolution No. (44) of 2023, including, but not limited to, obtaining a signed self-certification of their clients specifying details of all passports issued and held in their name(s). Virtual asset service providers can also use this as an opportunity to obtain all tax-related details in order to fulfill their international tax reporting obligations. Self-certification should not prevent virtual asset service providers from conducting appropriate due diligence.

Fifth Principle: Governance, Systems and Controls

189. **Governance Structure:** Virtual asset service providers are required to establish an appropriate governance structure, with a particular focus on IT governance. This should include developing and maintaining the necessary systems and controls to ensure full compliance with Money Laundering and the Financing of Terrorism regulations.

190. **Use of technologies and solutions:** The SCA expects virtual asset service providers to seek the use of their own or third-party technologies and solutions to meet their regulatory obligations, such as client risk assessment, fraud detection, transaction identification, monitoring and reporting, as well as risk management requirements.

191. **Transaction control and 'know your transaction' procedures:** Virtual asset service providers are expected to develop and implement effective transaction control systems to track the origin and destination of virtual assets and implement robust 'know your transaction' procedures that enable them to obtain detailed information about client transactions.

192. **Liability:** The Securities and Commodities SCA expects virtual asset service providers to act responsibly and with prudent care and not exploit their activities for illegal purposes. They must identify and effectively manage 'indicators' that may indicate illegal use of virtual assets.

193. **Selection of technical solutions:** While the SCA does not recommend specific providers or service providers on ongoing process control systems, virtual asset service providers shall ensure that the technical solutions used are appropriate and effective and conduct their own due diligence to ensure their efficiency and ability to mitigate virtual asset risks.

194. **Virtual Asset Compliance Control Program:** Virtual Asset Service Providers and compliance officers are expected to establish a compliance control program that includes carrying out periodic and effective internal audits.

195. **Appointment of a Money Laundering Reporting Officer (MLRO):** Virtual asset service providers are required to appoint a Money Laundering Reporting Officer, who is responsible for implementing and supervising the licensed body's compliance with anti-money laundering laws and regulations. In accordance with module 5 of the rulebook, the Money Laundering Reporting Officer must have an appropriate degree of seniority and independence to be effective in his role. This means that the MLRO must have the capacity and SCA to provide independent reports and make decisions based on his assessment of the risks associated with money laundering without interference or pressure from senior management. The role of the Money Laundering Reporting Officer is not only to coordinate the reporting of suspicious activities but also to continuously develop and update anti-money laundering programs and policies to align with changes in the legislative and regulatory environment.

Sixth Principle: Obligations to Report Suspicious Activities

196. Reporting obligations: Virtual asset service providers must fully familiarize themselves with their obligations under the rules on countering money laundering crimes, especially with regard to reporting suspicious activities or transactions. This means understanding when and how they need to report any activity believed to involve money laundering or terrorist financing.

197. Establishing contact with the Financial Information Unit: Before commencing any operations, the Securities and Commodities SCA expects virtual asset service providers to register on the state's Financial Information Unit (Go-AML) program that enables them to submit reports about suspicious activity and transaction.

198. Development of advanced transaction control systems: Virtual asset service providers are required to establish advanced transaction control systems to identify potential Money Laundering and the Financing of Terrorism activities. These systems must also be able to recognize any attempts to violate domestic and international sanctions. These systems can rely on new technological solutions, including the use of artificial intelligence and monitoring algorithms, to enhance their ability to identify and assess risks accurately and efficiently.

Seventh Principle: Lists of terrorism and the application of Security Council resolutions related to preventing and suppressing terrorism and its financing, stopping the spread of armaments and its financing, and relevant resolutions in the state.

199. Virtual asset service providers are required to thoroughly examine related transactions against international and domestic sanctions lists to ensure compliance with applicable sanctions regulations. This examination includes verifying the names of the parties involved in the transaction to ensure that they are not among the individuals or entities included in the aforementioned sanctions lists. In this regard, virtual asset service providers must:

- Conduct regular and continuous checks to verify the matching of names with sanctions lists.
- Update databases and examination systems periodically to reflect the latest changes in sanctions lists.
- Train their employees on how to recognize potential transactions that may violate sanctions rules.
- Develop and implement procedures to deal with transactions that identified in a match between the client, the originator of the transfer, or the beneficiary of the sanctions lists in order to freeze assets in accordance with the legislation in force in this regard.

Eighth Principle: Appropriate training

200. This principle requires virtual asset service providers to provide ongoing and effective training to all their employees to ensure full compliance with AML/CFT legislations and targeted financial sanctions legislations. This training must include:

- Introducing employees to current laws and regulations and how to apply the same in the context of their daily work.
- Training to identify suspicious activities and indicators that may indicate Money Laundering or Financing of Terrorism crimes.
- Periodically update employees about changes in internal policies and procedures and industry developments.
- Provide specialized training to employees working in sensitive areas such as compliance, client verification and transaction control.

Nineth Principle: Record keeping

201. Virtual asset service providers are required to follow effective record-keeping policies and procedures to ensure compliance with anti-Money Laundering and the Financing of Terrorism legislations. They are expected to maintain up-to-date records reflecting the obligations and due diligence applied thereto, and they shall be prepared to provide these records upon request by the Securities and Commodities SCA, and the records shall be kept for a period of not less than 10 years.

202. Transaction recording and Access to Information: The SCA recognizes that recording transactions for many virtual assets is linked to technologies such as Distributed ledger technology. It requires the development of special arrangements to ensure access to all information relating to transactions as needed, both for them and for the SCA.

203. Cash transaction controls: The SCA indicates that cash transactions in the virtual assets market involve high risks of Money Laundering and the Financing of Terrorism. Virtual asset service providers are required to implement enhanced controls to mitigate these risks, such as setting limits on cash deposits, prohibiting receiving cash directly, and ensuring that these controls are consistent with SCA's module 5 of the rulebook.

204. Due Diligence in day-to-day operations: All virtual asset service providers are expected to exercise utmost due diligence in their day-to-day operations and when dealing with clients. Their activities must be compatible with the rules for combating money laundering crimes to ensure that they are not exposed to regulatory risks or harm the reputation of the state's financial system 2017.

Submitting a licensing application

205. Applicants seeking a virtual assets license shall be willing to engage significantly with the SCA throughout the application process. The application process is generally divided into five stages, as follows:

- Due diligence and discussions with the SCA's team;
- Submission of the official application;
- Granting initial approval;
- Granting a license.
- License fees.

Due diligence and discussions with the SCA's team(s).

206. Before submitting an application, the license applicant is expected to provide the SCA with a clear explanation of its proposed business model and explain how it meets all of the SCA's applicable rules and requirements. This phase will also include the license applicant making a number of in-depth technical presentations, across all aspects of the proposed virtual asset activities. Given the complexity of the activities associated with the Virtual Assets Framework, a number of meetings between the license applicant and the SCA are likely required to be held.

Submission of the Official Application

207. Following discussions, and after the SCA feels reasonably satisfied that the license applicant's proposed business processes, technologies and capabilities are at a sufficiently advanced stage, the license applicant will be required to submit a completed Virtual Asset Application Form and supporting documents to the SCA. The fees stipulated on the application must also be paid.

Granting initial approval

208. The SCA will conduct an in-depth review of the application and supporting documents. The SCA will only consider granting initial approval to license applicants who are deemed able to adequately meet all applicable conditions and requirements.

Granting a license

209. Having confirmed that the license applicant has met all the conditions required for the activity, the SCA shall issue the seventh category license for the relevant activity. The license may be conditional on the license applicant fulfilling certain licensing requirements further in particular in relation to testing and operational capabilities of the license applicant and completing third party verification of the license applicant's systems where applicable.

210. Taking into account the increased risks associated with activities related to virtual assets, licensed bodies will be closely supervised by the SCA once they are licensed. Licensed bodies are expected to undergo ongoing assessments and must be prepared to undergo objective reviews from time to time.

License and renewal fees and commissions

211. For more information about the fees structure for VA activities you can visit the SCA's website in the below link[4].

[4]Regulations SCA's | Regulations | Securities and Commodities Authority