Model Law on Virtual Assets

The Commonwealth

Office of Civil and
Criminal Justice Reform

Introduction

Advancements in blockchain and distributed ledger technology have had a revolutionary impact across sectors, of which finance is the most notable. The efficiency, transparency and security of distributed databases has metamorphosed the way we transact and interact with people and systems. Like any technology, this technology has also resulted in concerns relating to financial security and market integrity. This has necessitated the creation of robust regulatory frameworks in financial, prudential and anti-money laundering and countering the financing of terrorism (AML/CFT) spheres across the globe.

Regulation of these technologies is particularly important for Commonwealth countries because there has been a large upswing in the adoption of Virtual Assets (as defined below at section 2(l)) in recent years in these countries. Emerging markets dominate the adoption of Virtual Assets globally. Some of the Commonwealth countries in the top 20 ranked countries in the recent "Geography of Cryptocurrency" report by Chainalysis were India, Pakistan, Nigeria, Canada, Bangladesh and the United Kingdom. Users in lower-middle and upper-middle income countries rely on Virtual Assets for remittances, and often even in preserving their savings in times of Fiat Currency volatility. At an institutional level too, investment in Virtual Assets is increasing rapidly - as of the end of Q4 of 2021, there were more than 860 Virtual Assets related funds across the globe with primary offices in more than 80 countries. We note that international bodies, such as the Financial Stability Board, the Financial Action Task Force (**FATF**), and the International Organization of Securities Commissions (**IOSCO**) have all called for the regulation of Virtual Assets and Virtual Asset Service Providers (**VASP**).

The domain of Virtual Assets also interfaces with other areas of law and technology. One such technology, that also significantly impacts financial markets, is artificial intelligence (**AI**). AI can analyze vast amounts of data at incredible speeds, predict market trends, optimize trading strategies, detect fraudulent activities, and enhance security measures in the Virtual Assets market. The growth of AI and automation presents both immense opportunities and challenges for Commonwealth member countries. As AI and automation continue to reshape financial markets, there is a growing need for regulatory frameworks to address potential risks, such as algorithmic biases and data privacy concerns, and understand how regulations governing AI interact with regulations governing Virtual Assets, and data protection, among others.

Given that these technologies are the inevitable future of the economy, this Model Law for Virtual Assets for Commonwealth member countries (**Model Law**) seeks to provide a regulatory framework that gives financial market actors much needed legislative clarity and protects customers.

A crucial step of this legislative journey - before full customisation and implementation of the Model Law by each Commonwealth member country - is having Commonwealth member countries agree on the purpose and scope of the Model Law. It will then be important to align definitions of key terms to ensure the industry has legal certainty and clarity. Commonwealth member countries will be able to trust that the governing rules across the Commonwealth will be uniform, and of the highest

standard. In this regard, the scope and purpose of this Model Law, as well as the way forward and the exclusions in the Model Law will be fundamental.

Another key focus of this Model Law for Virtual Assets is to mitigate money laundering (**ML**), terrorism financing (**TF**) and proliferation financing (**PF**) risks and incorporate the relevant FATF Recommendations for preventing ML, TF and PF. An important component of this would be the implementation of the FATF's "Travel Rule", which, at an elemental level, seeks to identify information on the sender and receiver in Virtual Asset transactions.

If Commonwealth member countries take advantage of the opportunity to modernise their regulatory frameworks, they would stimulate innovation and foster competition in their economies. The Model Law also has enormous potential to continue to advance the Commonwealth as a financial and technology network. A Commonwealth regulatory legal framework which is consistent across the 50+ countries will also likely serve as a benchmark for future regulation in other jurisdictions, influencing rulemaking around the world. An aligned regulatory and legal framework across Commonwealth member countries will provide much needed clarity for businesses of the future - including exchanges, trading platforms, brokers, custodians, as well as token and stable coin Issuers, non-fungible tokens (**NFTs**) creators - that intend to operate in the Commonwealth.

As the Commonwealth countries embark on the journey of establishing regulatory frameworks for Virtual Assets, a similar imperative arises in the rapidly evolving realm of AI, perhaps as a combined automation standard. Much like blockchain and distributed ledger technology, AI technologies are transforming industries, reshaping the workforce, and raising important ethical and legal questions. To address these challenges, it is essential for Commonwealth members to align on the purpose and scope of AI regulations. Defining key terms and harmonizing principles and technical standards are crucial steps in ensuring the responsible development and deployment of AI. Just as the scope and purpose of Virtual Asset regulations are fundamental, so too are the principles and standards governing AI, as they will play an integral role in shaping the future of technology and its impact on society.

While some countries have implemented regulatory regimes for Virtual Assets and VASPs, many jurisdictions have not yet put in place effective AML/CFT frameworks for mitigating the ML/TF/PF risks associated with Virtual Assets activities in particular. The rapid development, increasing functionality, growing adoption, and global, cross-border nature of Virtual Assets therefore makes the urgent action by countries to mitigate the ML/TF/PF risks presented by VA activities and VASPs. The use of Virtual Assets by ransomware networks is also a critical concern, and the growth of ransomware attacks has increased the importance of this effort to introduce effective AML/CFT frameworks globally.

The Model Law focuses on identifying and mitigating the risks associated with covered Virtual Assets activities, applying preventive measures, applying licensing and registration requirements, implementing effective supervision on par with the supervision of related financial activities and facilitating effective enforcement. In this regard, FATF Recommendations are relevant and have been considered in the drafting of this Model Law.

This Model Law is intended to assist member countries to adhere to the above requirements relating to the implementation of the Virtual Assets and VASP regime in their respective jurisdictions, as they deem appropriate.

Principles

This Model Law shall be based on the following guiding principles:

1. **Principle-Based:** The regulatory framework should be principle -based, outcome-focused and flexible to ensure that it is the least intrusive on innovation as possible. A light touch approach should be taken to avoid stifling the development of new technologies.
2. **Protection-Focused**: The regulatory framework should protect participants from counterparty risks and cover market integrity, surveillance, fair pricing, custody, clearing, disclosure of conflicts of interests, and systems and business continuity planning.
3. **Balanced and Proportionate:** The regulatory framework should balance the need for regulation with the need for protection. It should be proportionate to allow innovative firms in the development stages to succeed while ensuring financial stability and financial integrity in the market.
4. **Comprehensive:** The overall regulatory framework should be comprehensive, should factor the entire ecosystem of crypto technologies, and not merely be focussed on Virtual Assets. Even if the Model Law is limited in scope, Commonwealth countries should align on the way forward in terms of the regulatory next steps.
5. **Flexible and Adaptable:** The regulatory framework should be technology-neutral, flexible and take into account the regulatory readiness and resources of each country. It should not be prescriptive in terms of administrative requirements. Wherever possible, the Model Law should allow for Commonwealth countries to customise the framework, and provide more guidance by way of delegated legislation, such as implementing regulations. The sovereignty of Commonwealth member countries, and their ability to legislate independently should not be jeopardized.

Table of Contents

PART VII - MISCELLANEOUS

PART I - PRELIMINARY

1. Short title

This [Act] may be cited as the Virtual Assets Act [year].

For the consideration of the Commonwealth member countries:

Each jurisdiction may choose to name the law differently. Alternatively, a country may, instead of drafting a stand-alone law on virtual assets, choose to incorporate the provisions of this Model Law into existing laws or delegated legislation, including but not limited to laws governing Virtual Assets, Financial Services, ML/TF, among others.

2. Interpretation

(1) In this Act, unless a contrary intention appears:

For the consideration of the Commonwealth member countries:

The definitions contained in Section 2 of this Model Law are indicative. Commonwealth member countries may include more defined terms.

(a) **Beneficial Owner** means the Natural Person(s) who ultimately owns or controls a customer and/or the Natural Person on whose behalf a transaction is being conducted. It also includes those Persons who exercise ultimate effective control over a Legal Person or arrangement.

For the consideration of the Commonwealth member countries:

The concept of "control" may vary from jurisdiction to jurisdiction. Member countries may align this framework with the definition or interpretation of control under applicable local laws. According to the FATF, "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct
control.

(b) **Beneficiary** in relation to a transfer of Virtual Asset, means the Natural Person or Legal Person or the legal arrangement that will own the Virtual Asset on completion of the transfer.

(c) **Fiat Currency** means banknote or coin that is in circulation as a medium of exchange.

(d) **Initial Virtual Asset Offering** occurs when an Issuer makes a Virtual Asset publicly available for purchase or acquisition.

(e) **Issuer** means a person who issues Virtual Assets.

(f) **Legal Person** means any entity other than a Natural Person that can establish a permanent customer relationship with a financial institution or otherwise own property, and which is recognised in law by the [Jurisdiction]. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other entities that the Regulatory Authority may deem fit.

(g) **Natural Person** means an individual that conducts the relevant activity or operation listed in limbs (i)-(v) of the definition of a VASP under Section 2(1)(m) of this Act.

(h) **Originator**, in respect to a transfer of Virtual Asset, means the account holder who allows the transfer from that account, or where there is no account, the Natural Person or Legal Person that places the order with the originating VASP to perform the transfer.

(i) **Person** means a Legal Person or a Natural Person.

(j) **Politically Exposed Persons** means:

(i) Natural Persons who are or have been entrusted with prominent public functions by a foreign country, including Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of State-owned corporations and important political party officials,

(ii) Natural Persons who are or have been entrusted domestically with prominent public functions, for example Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of State-owned corporations and important political party officials,

(iii) Natural Persons who are or have been entrusted with a prominent function by an international organisation and includes members of senior management such as directors, deputy directors and members of the board or equivalent functions, and

(iv) family members and close associates of Natural Persons set out in subparagraphs (i) to (iii).

(k) **Regulatory Authority** means a body or agency established by or under a law of the [Jurisdiction] that grants or issues under that law or any other law licenses, permits, certificates, registrations, or other equivalent permissions, and performs any other regulatory function, including developing, monitoring, or enforcing compliance with standards or obligations prescribed by or under this [Act] or any other law in force in the [Jurisdiction].

(l) **Virtual Assets** mean a digital representation of value that may be digitally traded or transferred, and may be used for payment or investment purposes, but does not include a digital representation of Fiat Currencies, securities and other financial assets to the extent that they are regulated by other laws of the [Jurisdiction].

(m) **Virtual Asset Service Providers** or **VASP** means a Legal Person that, as a business, conducts one or more of the following activities or operations for or on behalf of another Person:

(i) exchange between Virtual Assets and Fiat Currencies;

(ii) exchange between one or more forms of Virtual Assets;

(iii) transfer of Virtual Assets;

(iv) safekeeping and/or administration of Virtual Assets or instruments enabling control over Virtual Assets;

(v) participation in, and provision of, financial services related to an Issuer's offer and/or sale of a Virtual Asset.

For the consideration of the Commonwealth member countries:

Notably, the act of using a software or technological stack for creating a Virtual Asset and a Virtual Asset Offering is not covered by the definition of a VASP. This Model Law strictly covers the concept of Initial Virtual Asset Offering.

However, Section 2 (m)(v) applies to participation in, and provision of, financial services or advice related to an Issuer's offer. To clarify, an entity engaged in placing a newly issued Virtual Asset for sale for the first time is a VASP, but the Issuer of the token itself is not.

Such an entity may be affiliated or unaffiliated with the Issuer undertaking the Initial Virtual Assets Offering. For example, this could include a business accepting purchase orders and funds and purchasing Virtual Assets from an Issuer to resell and distribute the funds or Virtual Assets, as well as book building, underwriting, market making and placement agent activity, etc.

For the purposes of this Section 2 (1)(m), "as a business" can be meant to exclude those who may carry out a function on a very infrequent basis for non-commercial reasons from being construed as VASPs. Generally speaking, a number of factors need to be taken into account in determining whether a person is carrying out an activity as a business. These may include:

- **Activity Itself:** the nature of the particular regulated activity that is carried on;
- **Commercial Motive**: the existence of a commercial element;
- **Marketing**: the act of holding oneself to be willing and able to engage in the regulated activity;
- **Solicitation:** the act of soliciting clients to offer them services falling under the regulated activity;
- **Scale:** the scale of the activity;
- **Proportion**: the proportion which the activity bears to other activities carried on by the person but which are not regulated; and
- **Continuity**: the degree of continuity of the above.

"Conducts" can mean to include the provision and/or active facilitation of a service, which refers to active involvement in the provision of activities covered under limbs (i)-(v) of the definition of a VASP

under this Section 2(1)(m).

(n) **White Paper** means a document prepared by the Issuer which meets the requirements of a white paper as set out in Section 31 (1) (a) of this [Act].

3. Objects of this Act

(1) The objects of this [Act] are to provide for the:

(a) legal basis for the establishment of VASPs and Issuers of Initial Virtual Asset Offerings in the [Jurisdiction];

(b) regulation of VASPs and Issuers of Initial Virtual Asset Offerings by the Regulatory Authority;

(c) registration or licensing of VASPs; and

(d) regulation of any other matters ancillary or connected to Virtual Assets and VASPs.

For the consideration of the Commonwealth member countries:

Notably, Section 3(1)(a) above **does not seek to regulate Virtual Assets, but VASPs and Issuers of, Virtual Assets**. This is because it may not be practicable to regulate Virtual Assets themselves. Further, Section 3(1)(c), is included with the intent that regulation of Issuers of Initial Virtual Asset Offerings, which may not be similar in form and manner as the regulatory regime applicable to VASPs, is not unduly encumbered with registration and licensing requirements.

Further, Commonwealth member countries may require VASPs **to be: (a) licensed or registered or both. This** flexibility has been codified in Section 3(1) (b). For reference, the FATF's Updated Guidance for a Risk-Based Approach to Virtual Assets and VASPs provides that countries may opt between to either have a licensing or registration regime or a mix of both. Accordingly, Section 3(1)(b) of this Model Law aims to ensure that each **Commonwealth member country can exercise their sovereignty, and take a decision based on their institutional readiness.**

Generally, the regulatory threshold for registration is lower than that for licensing. A licensing regime may be more prescriptive, and usually includes requirements around competence. For example, a licensing regime may require ensuring that a manager of a VASP has adequate experience and qualifications. In contrast, a registration may be accompanied mostly by reporting requirements. In any event, both licensing and registration regimes for Virtual Assets should include fit and proper requirements.

Licensing and registration may also co-exist. For example, the Regulatory Authority responsible for regulating VASPs may provide for licensing. However, additionally, to monitor AML/CFT related matters, the concerned regulator tasked with AML/CFT in the Commonwealth member country may require VASPs to register and comply with reporting requirements such as those applicable to financial institutions under existing AML/CFT laws. This may be done by way of delegated legislation.

Notably, this Model Law also envisages a scenario where there may not be a dedicated AML/CFT

law or similar regulatory framework in the Commonwealth member country. In such situations, AML/CFT related provisions may be brought within the remit of this Model Law itself, under Section 3(1)(d) above, which is an enabling residuary provision. **Such an enabling provision will also confer residuary powers to the Regulatory Authority or other authorities to monitor and supervise rapidly evolving regulatory concerns in the Virtual Assets ecosystem and adopt any measures necessary to regulate "connected matters" like money laundering and terrorism financing, customer protection concerns and general market integrity.**

The licensing and/or registration regime may be introduced and enforced by empowering the relevant Regulatory Authority or other authorities in the Commonwealth member country. An enabling provision in this regard has been codified in Section 3(1)(d). Details on the powers of the Regulatory Authority may be found in Part II of this Model Law.

(2) For the avoidance of doubt, this [Act] does not apply to the following:

(a) digital representations of value or rights that operates within a closed ecosystem of the Issuer, including but not limited to those:

(i) non-transferable outside a closed ecosystem,

(ii) non-exchangeable with real-world goods, services, discounts, purchases outside a closed ecosystem,

(iii) non-tradeable onwards on the secondary market outside of a closed ecosystem,

(iv) non-saleable on a secondary market outside of the closed loop-system,

(v) non-usable for payment or investment purposes, and

(vi) non-exchangeable for fiat-currency.

(b) digital representations of Fiat Currencies, securities and other financial instruments to the extent that they are regulated by other laws in the [Jurisdiction];

(c) digital representations of Fiat Currencies issued by the Central Bank of the [Jurisdiction], or any other jurisdiction; or

(d) any other digital representations of value or rights sought to be expressly excluded by the Regulatory Authority.

For the consideration of the Commonwealth member countries:

This Model Law, in line with FATF's definition, defines '*Virtual Assets*' as '*a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes*. 'Virtual Assets' definition does not include digital representations of Fiat Currencies, securities and other financial assets **that are already covered elsewhere in the laws of the jurisdiction.**

In line with the overall regulatory intent, it would be helpful if the Model Law explicitly states some exclusions to provide legislative clarity on the digital assets that fall outside the ambit of the Model

Law.

The Model Law seeks to exclude from the ambit of the law, tokens that are colloquially referred to as '**utility tokens'** (under Section3(2)(a)), **investment tokens** (under Section 3(2) (b)), **stablecoins,** that are digital representation of any Fiat Currency (under Section 3(2)(b)) and **CBDCs** (under Section 3(2) (c)). Additionally, under Section 3(2)(d), a discretionary provision has been included authorizing the Regulatory Authority to exclude any other digital representation of value or rights.

The reasoning for each of these exclusions is stipulated below:

Exclusion Under Section 3(2) (a)

Closed Loop Tokens

An example of a closed-loop token is a token that represents frequent flyer miles. These may be exchanged within the ecosystem for flight upgrades, but may not be traded on the secondary market, or otherwise transferred outside, or sold or exchanged for cash. Such tokens have limited utility and there may not be merit in regulating them.

Exclusion Under Section3(2) (b)

Investment Tokens

The second exclusion discusses "digital representations of Fiat Currencies, securities and other financial assets to the extent that they are regulated by other laws in the jurisdiction "

Investment tokens are tokens that: (i) confer rights and obligations that are substantially similar in nature to those conferred by a security (such as share or a debenture), derivative (such as futures and options) or other financial instrument (such as unit of a fund, commodity contracts or carbon credits); or (ii) has a substantially similar purpose or effect to a security (such as share or a debenture), derivative (such as futures and options) or other financial instrument (such as unit of a fund, commodity contracts or carbon credits). A Commonwealth member country may already have a regulatory regime for securities, derivatives, and such financial instruments and may choose to treat the Investment tokens in substantially similar nature. Accordingly, the phrase in ***Section3(2) (b)***which reads as – "*to the extent that they are regulated by other laws in the [Jurisdiction]*" – leaves the door open for Commonwealth member countries seeking to regulate Investment tokens to do so under their existing securities or sectoral laws. However, if a member country wishes to include Investment Tokens under the scope of this Model Law, it may, at its discretion, choose to expand the scope of this Model Law to digital assets inclusive of Investment Tokens and include related regulatory regime for Investment Tokens additionally.

Stablecoins

Stablecoins attempt to maintain a consistent exchange rate (or "peg") against another asset through a variety of mechanisms that usually, but not always, involve "collateralization" in the form of the Issuer holding reserved assets. If the underlying asset is a Fiat Currency issued either by the central bank of the concerned Commonwealth member country of the jurisdiction or issued by the central bank of any other jurisdiction, it may require separate regulatory intervention, depending upon

market readiness.

Just as in the case of investment tokens, the phrase in in ***Section 3(2) (b)***which reads as– "*to the extent that they are regulated by other laws in the jurisdiction*" – leaves the door open for Commonwealth member countries seeking to govern stablecoins under existing applicable laws. However, if a member country wishes to include Investment Tokens under the scope of this Model Law, it may, at its discretion, choose to expand the scope of this Model Law to digital assets inclusive of Investment Tokens and include related regulatory regime for Investment Tokens additionally.

Exclusion Under Section 3(2) (c)

CBDCs

Central Bank Digital Currency (**CBDCs)** are the digital form of Fiat Currency which has legal tender status in the concerned jurisdiction. It is regulated by its central bank (or prudential regulator). The digital form may or may not be cryptographically stored. Such instruments are excluded under the scope of this Model Law.

Exclusion Under Section 3(2) (d)

Tokens Excluded by Regulatory Authority

In addition to the tokens enlisted above, on a case-by-case basis, the Regulatory Authority may wish to exclude certain specific kind (or types) of tokens from the scope of this Model Law. For example, a token that represents rights over a real-world asset (such as real estate, art or antiques), may require different approach, which is distinct from other instruments. For such assets, the Commonwealth member countries may adopt a case-by-case approach. The language under Section 3(2)(d), vests upon the Regulatory Authority, the discretionary power to exclude any specific types of tokens.

PART II - REGULATORY AUTHORITY

4. Objectives of the Regulatory Authority

(1) The objectives of the Regulatory Authority are to –

(a) Endeavour to ensure financial stability in the [Jurisdiction].

(b) ensure the integrity of the Virtual Assets market in the [Jurisdiction];

(c) foster and maintain fairness, transparency and efficiency in the Virtual Assets sector in the [Jurisdiction];

(d) enhance and support the protection and fair treatment of customers; and

(e) prevent, detect and restrain conduct that causes or may cause damage to the reputation of the [Jurisdiction].

(2) In achieving its objectives and performing its functions below in Section 5, the Regulatory Authority must take into take into account the need for a primarily risk-based, pre-emptive and outcomes focused approach, and prioritise the use of its resources in accordance with the significance of risks to the achievement of its objective.

5. Functions of the Regulatory Authority

(1) In achieving its objectives, the Regulatory Authority shall perform the following functions:

(a) to register or license VASPs and Initial Virtual Asset Offerings in the [Jurisdiction];

(b) to regulate and monitor VASPs and Initial Virtual Asset Offering in the [Jurisdiction];

(c) to prepare and maintain a register of VASPs and Issuers of Initial Virtual Asset Offering in the [Jurisdiction];

(d) to issue, publish and implement, from time to time, [delegated legislation] in connection with the [Act];

(e) to ensure VASPs comply with requirements to combat money laundering and terrorism financing in the [Jurisdiction];

(f) to identify and assess money laundering and terrorism financing risks emerging from Virtual Asset activities and the activities or operations of VASPs, and apply a risk-based approach to mitigating those risks;

(g) to identify Natural Person or Legal Persons that carry out VASP activities without the requisite licence or registration and apply appropriate sanctions to them;

For the consideration of the Commonwealth member countries:

Section 5(1)(d) allows the Regulatory Authority to issue and publish rulebooks, notices, guidelines, guidance notes, circulars and any other similar instrument under this Model Law, which addresses, any matters:

i. in connection with any Virtual Assets in the country;

ii. in connection with any VASPs or Initial Virtual Asset Offerings in the country; and

iii. regarding the interpretations and enforcements of this Model Law.

In this regard, Commonwealth member countries may refer to the work of international organisations such as FATF, FSB, BIS, IOSCO, among others.

Further, Sections 5(1)(e) – (g) above assume that AML / CFT laws may vary from jurisdiction to jurisdiction. While some may have dedicated AML/CFT regulatory bodies or authorities, others may still be in the process of developing regulatory frameworks. Section 5(1)(e) above provides an enabling provision and gives the Commonwealth member countries the flexibility to: (a) either introduce delegated legislation and assign the role of compliance with AML/CFT provisions to the Regulatory Authority under this Model Law, or (b) engage with the concerned AML/CFT regulator.

For example, in the absence of a dedicated AML/CFT regulator, the Regulatory Authority may:

i. subject VASPs to risk-based supervision or monitoring; and

ii. require VASPs and Issuers of Initial Virtual Asset Offering in the jurisdiction to comply with the full range of AML/CFT preventive measures and targeted financial sanctions obligations.

Further, under Section 5(1)(b) and Section 5(1)(g) above, the Regulatory Authority, would be empowered to issue sanctions.

In performing its functions under Sections 5(1)(e) to (g), the Regulatory Authority may establish guidelines, and provide feedback, which will assist VASPs in applying national measures to combat money laundering and terrorism financing, and in detecting and reporting suspicious transactions.

(h) to facilitate innovation and development of the Virtual Assets sector;

(i) to establish a regulatory sandbox to provide a limited environment for emerging activities related to Virtual Assets which do not fall into the definitions of the existing VASPs;

(j) to promote customer awareness and education in respect of matters provided for under this [Act];

(k) to undertake such other functions as may be conferred on it under this [Act] or any other law in force in the [Jurisdiction]; and

(l) to regulate any other matters ancillary or connected to Virtual Assets and VASPs in the [Jurisdiction].

For the consideration of the Commonwealth member countries:

Section 5 (1) (k) and (l) provide enabling provisions for the Commonwealth member countries to regulate emerging products and services with the Virtual Assets sector. This may include Decentralised Finance, Decentralised Autonomous Organisations, stablecoins, among others. The aim of these provisions is to allow Commonwealth member countries to decide the extent to which they may regulate the Virtual Assets sector, given their market readiness and regulatory preparedness.

6. Powers of the Regulatory Authority

(1) The Regulatory Authority shall have the:

(a) power to issue, suspend, revoke or alter a VASP license;

(b) power to promulgate any [delegated legislation] to supplement the provisions of this [Act];

(c) power to issue [delegated legislation] to supplement the provisions of this [Act];

(d) power to provide exemptions under this [Act];

(e) power to adopt any measures that it deems necessary, in its sole discretion, for or in connection with, or reasonably incidental to, performing its functions in accordance with this [Act]; and

(f) any other powers as conferred, or expressed to be conferred, on it by or under:

i. this [Act]; and/or

ii. any other law in force in the [Jurisdiction].

For the consideration of the Commonwealth member countries:

Section 4 has been drafted as an enabling provision. Commonwealth member countries may include any additional powers to allow the Regulatory Authority to perform the functions in Section 3 above.

For example, given the inherent transnational nature of the Virtual Assets industry, FATF expects countries to rapidly provide the widest possible range of international cooperation in relation to money laundering, predicate offences, and terrorist financing relating to Virtual Assets. Accordingly, the Commonwealth member countries may add a legal basis for exchanging information with their foreign counterparts through an explicit power under this Section.

PART III - LICENSING OR REGISTRATION OF VASPS

7. VASPs to be licensed

(1) A Natural Person shall not provide Virtual Asset services as a business in the [Jurisdiction].

(2) A Legal Person shall not provide Virtual Asset services as a business in the [Jurisdiction], unless the Legal Person is licensed from or registered with the Regulatory Authority as a VASP

For the consideration of the Commonwealth member countries:

This provision implies that Commonwealth member countries are required, at a minimum, to license or register VASPs in their jurisdiction. Whilst licensing or registration are different approaches, either approach may be adopted by them, depending on the regulatory appetite and market readiness in their jurisdiction.

Notably, Part III of this Model Law has been drafted assuming that Commonwealth member countries may choose to prescribe a licensing framework. Specifically, **Section 7 onwards, the provisions provide the procedural requirements for obtaining a VASP license. If Commonwealth member countries choose to provide a registration process, they may tailor this segment accordingly.**

Commonwealth member countries may also consider including an optional provision that allows countries to license/register VASPs that offer services/products to customers in or conduct operations from a foreign jurisdiction (i.e., cross-border). As a matter of policy, it would be good to cover both possibilities in this Model Law and include an explanatory note that jurisdictions may choose to cover the latter.

8. Virtual Asset activities that may be provided

(1) An applicant may apply for a licence to operate as a VASP conducting any one or more of the following activities:

(a) exchange between Virtual Assets and Fiat Currencies;

(b) exchange between one or more forms of Virtual Assets;

(c) transfer of Virtual Assets;

(d) safekeeping and /or administration of Virtual Assets or instruments enabling control over Virtual Assets;

(e) participation in, and provision of, financial services related to an Issuer's offer and sale of a Virtual Asset;

(f) any other activities related to Virtual Assets that the Regulatory Authority may from time to time include.

For the consideration of the Commonwealth member countries:

The definition of a VASP at present includes the activities set out at above from (a) to (e). While (a), (b) and (c) may be provided by Virtual Assets broker-dealers and exchanges, (d) may be provided by Virtual Assets custodians, and (e) may allow an Issuer of Virtual Asset Offerings to offer their Virtual Assets for sale for the first time.

As the ecosystem evolves, Commonwealth member countries may seek to also regulate other activities related to Virtual Assets, such as Virtual Assets collective investment funds, decentralised finance platforms, among others. Section 8 (1)(f) above provides an enabling framework for this. Notably, this residual provision is not included in the definition of a VASP in the definitions.

Further, Commonwealth member countries may by way of delegated legislation explain the scope of activities undertaken under each of the above. They may also specify additional obligations for each of the activities above, beyond those envisaged under Section 16 below, which is applicable to each VASP.

9. Application to carry on business as a VASP

(1) A Legal Person who proposes to carry on business as a VASP shall apply to the Regulatory Authority and obtain a licence.

(2) Each of the Beneficial Owners of an applicant shall be fit and proper to perform duties, as may be prescribed.

(3) The application shall be in the form prescribed by the Regulatory Authority from time to time.

10. Assessment, issuing or refusing a VASP licence application

(1) The Regulatory Authority shall consider a licence application and any additional information and documents received from an applicant.

(2) The Regulatory Authority shall, within a reasonable period of time:

(a) accept the application and designate the applicant as a VASP;

(b) reject the application, and provide the reasons for refusing to grant its approval; or

(c) request the VASP to provide additional information within the time-period stipulated by the Regulatory Authority. If the VASP fails to comply with the request for additional information within the time stipulated under this Act, the application shall be deemed to be withdrawn. For the avoidance of doubt, once additional information requested by the Regulatory Authority is received, the information forms part of the application and the application is considered to be a complete application.

(3) The Regulatory Authority may refuse to grant a licence to an applicant for a VASP licence on any one or more grounds:

(a) where the applicant has not furnished to the Regulatory Authority such information relating to the applicant, and to any circumstances likely to affect the applicant's method of conducting business, as may be prescribed, being information verified in such manner, whether by statutory declaration or otherwise, as the Regulatory Authority may require;

(b)if the information supplied by the applicant is not complete, false or misleading;

(c)where the Regulatory Authority is not satisfied that the business will be financially viable, or the funds used to pay the capital of the applicant is acceptable;

(d) if there is reason to believe that the applicant would not comply, or be able to comply, with the requirements of this [Act];

(e) if the applicant or its officers are not fit and proper to carry on business as a service provider and to provide the services described in the application;

(f) if any Beneficial Owner or person holding a significant or controlling interest in the applicant is not fit and proper;

(g) where the applicant has not paid the prescribed fee to the Regulatory Authority;

(h) if the services to be provided by the applicant will be provided in a manner that will or is likely to bring the [Jurisdiction] into disrepute;

(i) if the granting of the application will or is likely to be contrary to public interest; or

(j) for any other reason that the Regulatory Authority may deem fit.

(4) The Regulatory Authority shall, as soon as practicable after a licence has been issued to the applicant, include in the register the following details:

(a) the name and address of the VASP;

(b) the services that may be provided by the VASP by way of the licence;

(c) the licence number; and

(d) the time period for which the licence is valid.

11. VASP licence issued by the Regulatory Authority

(1) A VASP licence issued by the Regulatory Authority shall be in the form specified by the Regulatory Authority and state the following:

(a) the name and address of the VASP;

(b) the fact that the VASP licence has been issued;

(c) the services that may be provided by way of the licence;

(d) the licence number; and

(e) the time period for which the licence is valid.

(2) A VASP shall prominently display its licence on or at all places where it provides its services as a VASP, including physical business premises and online.

For the consideration of the Commonwealth member countries

Commonwealth member countries may allow Regulatory Authorities to provide conditional licenses.

Before imposing conditions on a licence, the Regulatory Authority may give the licensee notice in writing of the conditions it proposes to impose and the reasons for the conditions.

The licensee may after receiving the notice, give the Regulatory Authority reasons why the Regulatory Authority should not impose the conditions.

12. Term and renewal of VASP licence

(1) A licence for a VASP shall remain in force until it is expired, suspended or revoked under this [Act].

(2) A VASP may not assign or transfer a licence. Any purported assignment or transfer of a VASP licence shall be of no effect and will be void.

(3) A VASP shall pay the prescribed fee to the Regulatory Authority on or before each anniversary of the date of issue of the VASP licence.

13. Suspension of VASP licence

(1) The Regulatory Authority may serve a notice of non-compliance to a VASP, if the Regulatory Authority is satisfied that:

(a) there is a breach of a provision of the [Act] or its accompanying [delegated legislation];

(b) the Regulatory Authority considers that the Beneficial Owner(s) of the VASP are not fit and proper persons under this [Act];

(c) the Regulatory Authority is furnished, by or on behalf of the VASP, with information, which is false, inaccurate or misleading;

(d) the VASP has obtained the VASP licence by making false statements or by any other irregular means; or

(e) the VASP has not commenced the Virtual Asset business that it is authorised to provide within 12 months, from the date of issue of the licence, or has ceased to provide the Virtual Asset service; or

(f) the Regulatory Authority considers it desirable to suspend or revoke the licence for the protection of customers and the public;

(h) for any other reason determined by the Regulatory Authority.

(2) A notice of non-compliance shall specify:

(a) the provision of the [Act] or its accompanying [delegated legislation] that was breached;

(b) the penalty payable under the licence;

(c) the period within which a penalty must be paid; and

(d) the period within which a breach is to be rectified.

(4) If a VASP fails to rectify the breach of the licence or fails to pay the penalty within the period specified in the notice, the Regulatory Authority shall:

(a) suspend the licence; and

(b) serve a notice of suspension to the VASP; and

(c) allow the VASP to provide reasons why the licence should not be revoked.

(5) Subject to Section 13(4), all operations shall cease until the Regulatory Authority advises the VASP that the suspension is lifted.

(6) If a VASP fails to comply with Section 13(4)(c), the Regulatory Authority shall revoke the VASP licence, and the Regulatory Authority must serve a notice of the revocation to the VASP.

14. Alteration or revocation of VASP licence

(1) The Regulatory Authority may alter or revoke a VASP licence, if:

(a) the Regulatory Authority is satisfied that:

i. the applicant or VASP has engaged in or facilitated serious criminal offences, including but not limited to money laundering or terrorism financing;

ii. a Beneficial Owner of the applicant or VASP is not fit and proper to fulfil the responsibilities; or

i. by reason of the applicant or the VASP, or any Natural Person employed by, or associated with, the applicant or the VASP for the purposes of his business:

A. has been convicted within the [Jurisdiction] of an offence;

B. has been convicted of an offence under this [Act]; or

C. has committed a breach of any rules made by the [Minister or Regulatory Authority] under this [Act] for regulating the conduct of business by holders of licences; or

(b) the VASP is no longer fit and proper to hold a license; and

(c) the VASP is not complying with this [Act] in a material manner.

(d) The VASP requests the Regulatory Authority to alter or revoke their license.

For the consideration of the Commonwealth member countries

Before refusing, suspending or revoking a licence under this Act, the Regulatory Authority may decide, by way of delegated legislation, to give the applicant or Licensee concerned notice in writing of his or her intention so to do specifying therein the grounds on which he/she proposes to refuse, suspend or revoke the licence.

The Regulatory Authority may afford the applicant or the licensee, as the case may be, an opportunity of submitting to him a written statement of representations against or objections to the proposed refusal, suspension or revocation, within such time as may be specified by the Regulatory Authority.

15. Register of VASPs

(1) The Regulatory Authority shall maintain a publicly available Register of licensees.

(2) The Register shall contain:

(a) the VASPs name and place of business; and

(b) the services the VASP is authorised by the licence to provide;

(c) the licence number of the VASP;

(d) the time period for which the licence is valid; and

(e) any other information as prescribed by the [delegated legislation]

(3) The Regulatory Authority shall make the register available for inspection by the public.

16. Obligations of VASPs

A VASP shall at all times, in the manner prescribed by the Regulatory Authority from time to time:

(a) provide its services honestly and fairly;

(b) maintain and hold the prescribed capital specified by the Regulatory Authority;

For the consideration of the Commonwealth member countries:

We recommend that VASPs hold sufficient capital to ensure market integrity and operational resilience. The Regulatory Authority may prescribe minimum values for paid up capital, operational capital and reserves, based on the economic underpinnings of each jurisdiction.

Generally, the capital requirement may be prescribed as the higher of [absolute value] or [insert percentage] % of fixed annual overheads.

Further, the capital requirements may vary by activity. For example, for an entity offering "safekeeping and /or administration of Virtual Assets or instruments enabling control over Virtual Assets" (a custodian), the capital requirement may be higher than that for a broker-dealer offering "exchange between Virtual Assets and Fiat Currencies".

The requirements should also factor in scenarios where the same VASP provides more than one service.

(c) manage any actual and potential conflicts of interest related to its services;

(d) manage and mitigate any actual and potential risks associated with its services;

(e) have adequate technological, financial and human resources to discharge its services;

(f) comply with the full range of AML/CFT preventive measures, including targeted financial sanctions obligations;

(g) have its annual financial statements audited;

(h) ensure that recording, storing, protecting and transmission of the data processed by it is in accordance with the applicable laws in the [Jurisdiction];

(i) ensure that all marketing and promotional materials are fair, clear, transparent and not misleading;

(j) plan for business continuity and disaster recovery in the event of an incident or a disaster;

(k) have in place a mechanism for handling customer complaints;

(l) have in place a mechanism for protecting whistle-blowers;

For the consideration of the Commonwealth member countries:

Commonwealth member countries may already have whistle-blower protection laws in force in their countries. This provision allows countries that may not have such laws to bring whistle-blower protection under the ambit of this Model Law, in the manner they deem fit.

(m) take reasonable steps to prevent market abuse and ensure the integrity and transparency of financial markets;

(n) take reasonable steps to ensure its representatives (employees and persons acting on its behalf) comply with the law;

(o) maintain competence to provide the Virtual Asset services;

(p) if offering for sale a Virtual Asset, conduct due diligence on the Virtual Asset and its issuer, taking into account the requirements of a White paper, as set out in Section 31(1)(a).

For the consideration of the Commonwealth member countries

Market abuse includes any manipulative or deceptive practices that may distort market prices, undermine confidence, or create unfair advantages for certain market participants. Commonwealth member countries may, in line with existing laws on preventing market abuse, issue delegated legislation to elaborate on what market abuse may entail, and how it may be checked. Some prohibited practices may include, among others,

- **Pump and Dump Schemes:** Individuals or groups artificially inflate the price of a Virtual Asset by spreading positive information (pumping) and then quickly sell off their holdings at the inflated prices (dumping).
- **Insider Trading:** Trading Virtual Assets based on non-public information, such as upcoming partnerships, regulatory decisions, or technological developments.
- **Wash Trading:** A trader buys and sells a Virtual Asset to create artificial trading volume without any change in ownership.
- **Spoofing and Layering:** Placing large buy or sell orders with the intention of cancelling them before execution (spoofing) or placing multiple deceptive orders to create a false sense of market demand (layering).
- **Front Running:** Executing trades on advance knowledge of upcoming transactions before carrying out those transactions on behalf of clients.

(q) take reasonable steps to ensure that its Beneficial Owners are fit and proper;

(r) take reasonable steps to ensure that its Beneficial Owners or any Natural Person employed by, or associated with, the VASP comply with this [Act] and all applicable laws in the [Jurisdiction];

(s) take reasonable steps to ensure that its Beneficial Owners or any Natural Person employed by, or associated with, the VASP comply with the code of conduct for VASPs set out by the Regulatory Authority from time to time;

(t) take reasonable steps to ensure that its Beneficial Owners or any Natural Person employed by, or associated with, the VASP comply with the conditions of the licence issued by the Regulatory Authority; and

(u) take reasonable steps to ensure that its Beneficial Owners or any Natural Person employed by, or associated with, the VASP are competent to provide the services of the VASP.

For the consideration of the Commonwealth member countries:

Commonwealth member countries may consider codifying specific additional obligations for each of the activities covered under Section 8, beyond that are applicable to all VASPs under Section 16.

These obligations may be imposed such that they are: (1) regulation-led, that is, prescribed the Regulatory Authority by way of delegated legislation, or (2) industry-led, that is adopted voluntarily by the industry.

For example, a VASP providing safekeeping and /or administration of Virtual Assets or instruments enabling control over Virtual Assets, may be subject to the following technical standards set forth by the Cryptocurrency Certification Consortium (C4):

- The cryptographic keys are created by the actor who will be using it.
- A digital signature for the key creation software is generated, published, and validated prior to each execution.
- In cases where an automated agent will make use of a cryptographic key, it is required that the administrator of that system generates the key/seed on a suitable offline system with sufficient entropy, have this key/seed transferred securely onto the target device, and then securely deleted using Cryptocurrency Security Standard (CCSS)-compliant data sanitization techniques to protect the confidentiality of the key/seed.
- The key or seed generation methodology is validated prior to use. Software does not include features that restrict which values can be used. Software does not include features that store or transmit data to another actor, unless that feature enhances security.
- In cases where keys or seeds are created without the use of software (e.g., dice, a deck of cards, or other non-digital source of entropy), the creation methodology must be validated to ensure determinism is not present (e.g., there are no weighted dice, each card in the deck is unique).

- The key or seed is generated using either a (1) Deterministic Random Bit Generator (DRBG) that conforms to NIST SP 800-90A, and has been seeded with at least two separate cryptographically secure sources of entropy that have been combined in a cryptographically secure manner (e.g., SHA256[UnguessableFactor1 + UnguessableFactor2]) or (2) a Non-deterministic Random Bit Generator (NRBG), or a "True Random Number Generator" (TRNG) that passes industry-standard statistical tests for randomness such as DIEHARD, Crypt-X, or NIST STS. The Dual_EC DRBG has been demonstrated to be vulnerable and thus must not be used.
- The cryptographic keys and seeds are created on a system with sufficient entropy to ensure the keys are not created with any bias towards a reduced range of values, or other deterministic properties.
- Any address generated by a wallet must require a minimum of 2 signatures (commonly referred to as a multi-sig wallet) in order to spend funds, where a separate actor holds each signing key. The actors can either be human or system (i.e. two humans, two systems, or one human and one system) but must be separate entities that each manage their own key for the wallet.
- Redundant keys are assigned to each wallet for recovery purposes.
- Any keys that have signing authority on a single wallet must be stored in different locations.
- A backup must exist for at least as many keys as are required to spend funds. The backup must be protected against environmental risks such as fire, flood, and other acts of God. The backup key/seed must be stored in a location that is geographically separate from the usage location of the primary key/seed.

17. Appointment of a Director/Authorised Representative

(1) A VASP shall appoint a Director or authorised representative, who shall be responsible for the functioning of the VASP in the [Jurisdiction].

(2) A VASP shall ensure that the Director is fit and proper.

(3) A VASP who intends to appoint a Director must apply to the Regulatory Authority for its approval.

(4) The Regulatory Authority may from time to time prescribe the functions of the Director.

(5) The Regulatory Authority may from time to time prescribe the eligibility criteria for Natural Persons applying to become a Director of Virtual Asset Services Provider in the [Jurisdiction].

For the consideration of the Commonwealth member countries:

Each Commonwealth member country may expand on the corporate governance requirements and elaborate on this section.

Each Commonwealth member country may, at its discretion, determine the citizenship and/or residency requirements of the Director. This may be done by way of delegated legislation. For example, the Regulatory Authority may prescribe that a citizen or non-citizen shall be eligible to be appointed as a Manager. Further, in the case of a non-citizen, the individual must have resided in the jurisdiction for a specified time period (say 6 consecutive months).

Further, in addition to fitness and propriety requirements and/or citizenship / residency requirements, each Commonwealth member country may prescribe other eligibility criteria for Directors, such as minimum experience in the domain of Virtual Assets.

PART IV - PREVENTION OF MONEY LAUNDERING AND TERRORISM FINANCING BY VASPS

For the consideration of the Commonwealth member countries:

Part IV of this Model Law, read with Section 3(1)(d) assumes that the Commonwealth member country does not have AML/CFT laws. It provides dedicated preventative measures for VASPs from an AML/CFT lens.

If the Commonwealth member country already has an AML/CFT law, it may amend or modify this Section to read harmoniously with the law. Further, the member countries may seek to issue VASP specific AML/CFT measures, as prescribed by FATF, and codified in Part IV of the Model Law below.

18. Appointment of a Money Laundering Reporting Officer

(1) A VASP shall appoint a Money Laundering Reporting Officer, who shall be responsible for complying with the full range of AML/CFT preventive measures, including targeted financial sanctions obligations the VASP in the [Jurisdiction].

(2) A VASP shall ensure that the Money Laundering Reporting Officer is fit and proper.

(3) A VASP who intends to appoint a Natural Person as a Money Laundering Reporting Officer must apply to the Regulatory Authority for its approval.

(4) The Regulatory Authority may from time to time prescribe the functions of the Money Laundering Reporting Officer.

(5) The Regulatory Authority may from time to time prescribe the eligibility criteria for Natural Persons applying to become a Money Laundering Reporting Officer of VASP in the [Jurisdiction].

For the consideration of the Commonwealth member countries:

Each Commonwealth member country may take a call on the citizenship and/or residency requirements of the Money Laundering Reporting Officer. This may be done by way of delegated legislation. For example, the Regulatory Authority may prescribe that a citizen or non-citizen shall be eligible to be appointed as a Manager. Further, in the case of a non-citizen, the individual must had resided in the jurisdiction for a specified time period (say 6 consecutive months).

Further, in addition to fitness and propriety requirements and/or citizenship / residency

requirements, each Commonwealth member country may prescribe other eligibility criteria, such as minimum experience in the domain of Virtual Assets.

19. Risk assessment

(1) Every VASP shall—

(a) take appropriate measures to identify, assess and understand its money laundering and terrorist financing risks in relation to—

(i) its customers;

(ii) the countries or jurisdictions of its operations; and

(iii) its products, services, transactions and delivery channels;

For the consideration of the Commonwealth member countries:

As part of the FATF's fifth round of mutual evaluations, countries will be expected to require VASPs to take appropriate steps to identify, assess, manage and mitigate their money laundering, terrorist financing and proliferation financing risks.

The nature and extent of any assessment of proliferation financing risks should be appropriate to the nature and size of the business. Obliged entities should always understand their proliferation financing risks, but competent authorities may determine that individual documented risk assessments are not required, provided that the specific risks inherent to the sector are clearly identified and understood. Please refer to: https://www.fatf-gafi.org/en/publications/Mutualevaluations/5th-Round-Methodology.html

(b) develop and implement a comprehensive risk management system approved by the VASP's senior management and commensurate with the scope of its activities, incorporating continuous identification, measurement, monitoring and controlling of identified risks;

(c) take appropriate measures to manage and mitigate those risks referred to in paragraph (a) above; and

(d) take account of any risk assessment carried out at a national level and any regulatory guidance issued by its Regulatory Authority or any other regulatory body in the [Jurisdiction]

(2) Every VASP shall carry out a risk assessment —

(a) prior to the launch of a product or business practice;

(b) prior to the use of new or developing technologies:

(c) when there is a major event or development in the management and operation or the group, to identify and assess the identified risks that may arise in relation to such products, business practices or technology for both new and pre-existing products and such assessment shall take into account—

(i) customer, country or geographic area, product, service, transaction, and means of delivery risk factors, which shall be proportionate to the nature and size of the financial institution's business; and

(ii) the outcome of any risk assessment carried out at a national level, and any regulatory guidance issued.

(3) Every VASP shall document in writing the outcome of its risk assessment and shall keep the same up to date and make it available to the Regulatory Authority upon request.

20. Customer due diligence

(1) Every VASP shall undertake customer due diligence (CDD) measures when opening an account for or otherwise establishing a business relationship with a customer.

(2) VASPs shall undertake CDD measures when:

(a) doubts exist about the veracity or adequacy of previously obtained identification information of a customer;

(b) there is a suspicion of activities relating to identified money laundering and terrorism financing risks involving the customer or the customer's account;

(c) a person, who is neither a customer nor in an established business relationship with the VASP wishes to carry out a transaction (to be referred to as an "occasional transaction").

For the consideration of the Commonwealth member countries

The occasional transactions designated threshold above which VASPs are required to conduct CDD as per the FATF is USD/EUR 1000. We recommend that Commonwealth member countries subscribe uniformly to this threshold.

(3) VASPs shall identify the customer (whether permanent or occasional, and whether Natural Person or Legal Person or legal arrangement) and verify that customer’s identity using reliable, independent source documents, data or information (identification data).

(4) VASPs shall verify that any person purporting to act on behalf of the customer is so authorised and identify and verify the identity of that person.

(5) VASPs shall identify the Beneficial Owner and take reasonable measures to verify the identity of the Beneficial Owner, using the relevant information or data obtained from a reliable source, such that the VASP is satisfied that it knows who the Beneficial Owner is.

(6) VASPs shall take steps to understand and, as appropriate, obtain information on, the purpose and intended nature of the business relationship.

(7) VASPs shall conduct ongoing due diligence on the business relationship, including:

(a) scrutinising transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the VASP's knowledge of the customer, their business and risk profile, including where necessary, the source of funds; and

(b) ensuring that documents, data, or information collected under the CDD process is kept up-to-date and relevant, by undertaking reviews of existing records, particularly for higher risk categories of customers.

(8) For customers that are Legal Persons or arrangements, the VASP shall take steps to understand the nature of the customer's business and its ownership and control structure.

(9) For customers that are Legal Persons or arrangements, the VASP shall identify the customer and verify its identity through the following information:

(a) for customers that are Legal Persons, the VASP shall identify and take reasonable measures to verify the identity of Beneficial Owners through the following information:

(i) the identity of the Natural Person(s) (if any) who ultimately has a controlling ownership interest in a Legal Person.

i. (ii) to the extent that there is doubt under (i) as to whether the person(s) with the controlling ownership interest is the Beneficial Owner(s) or where no Natural Person exerts control through ownership interests, the identity of the Natural Person(s) (if any) exercising control of the Legal Person or arrangement through other means.

(iii) where no Natural Person is identified under (i) or (ii) above, the identity of the relevant Natural Person who holds the position of senior managing official.

(b) for customers that are legal arrangements, the VASP shall identify and take reasonable measures to verify the identity of Beneficial Owners through the following information:

(i) for trusts, the identity of the settlor, the trustee(s), the protector (if any), the beneficiaries or class of beneficiaries, and any other Natural Person exercising ultimate effective control over the trust (including through a chain of control/ownership).

(ii) for other types of legal arrangements, the identity of persons in equivalent or similar positions.

(10) VASPs shall verify the identity of the customer and Beneficial Owner before or during establishing a business relationship or conducting transactions for occasional customers; or (if permitted) may complete verification after the establishment of the business relationship, provided that:

(a) this occurs as soon as reasonably practicable.

(b) this is essential not to interrupt the normal conduct of business; and

(c) the money laundering and terrorism financing risks are effectively managed.

(11) VASPs shall adopt risk management procedures concerning the conditions under which a customer may utilise the business relationship prior to verification.

(12) VASPs shall apply CDD requirements to existing customers based on materiality and risk, and to conduct due diligence on such existing relationships at appropriate times, considering whether and when CDD measures have previously been undertaken and the adequacy of data obtained.

(13) VASPs shall perform enhanced due diligence where the money laundering and terrorism financing risks are higher.

(14) VASPs shall apply simplified CDD measures where lower risks have been identified, through an adequate analysis of risks by the country or the VASP. The simplified measures should be commensurate with the lower risk factors but are not acceptable whenever there is suspicion of money laundering and terrorism financing risks, or specific higher risk scenarios apply.

(15) Where a VASP is unable to comply with relevant CDD measures:

(a) it shall not to open the account, commence business relations, or perform the transaction; or should terminate the business relationship.

(b) it shall consider making a suspicious transaction report (STR) in relation to the customer.

(16) In cases where VASPs form a suspicion of money laundering or terrorist financing, and they reasonably believe that performing the CDD process will tip-off the customer, the VASP shall not pursue the CDD process, and instead shall file a STR.

(17) VASPs shall keep all relevant information accurate current and in accordance with the provisions of this [Act].

(18) VASPs shall comply with any additional [delegated legislation] put in place by the [Regulatory Authority] under this [Act].

21. Record keeping

(1) VASPs shall maintain all necessary records on transactions, domestic and international, for at least [5 years] following completion of the transaction.

(2) VASPs shall keep all records of all information obtained through CDD measures, including account files and business correspondence and copies of all documents evidencing the identity of customers and Beneficial Owners, and the results of any analysis undertaken in accordance with the provisions of this Act, all of which shall be maintained for at least [5 years] following the termination of the business relationship or after the date of the occasional transaction.

(3) Transaction records should be sufficient to permit reconstruction of individual transactions to provide, if necessary, evidence for prosecution of criminal activity.

(4) VASPs shall ensure that all CDD information and transaction records are made available swiftly to the Regulatory Authority, or any other regulatory body in the [Jurisdiction] when requested.

(5) All records shall be kept in written form in [English] language, or in a form readily accessible and convertible in written form in the English language.

(6) VASPs shall ensure that all records (including their copies) retained by that VASP pursuant to any provision of Part IV of this [Act] are destroyed as soon as practicable after the expiry of the period of [5 years] VASP is required to retain that record, unless there is a lawful reason for retaining a record under other applicable laws in the [Jurisdiction].

22. Politically Exposed Persons (PEPs)

(1) In relation to foreign PEPs, in addition to performing the CDD measures required under Section 20, VASPs shall:

(a) put in place risk management systems to determine if a customer or Beneficial Owner is a PEP;

(b) obtain senior management approval before establishing (or continuing, for existing customers) such business relationships;

(c) take reasonable measures to establish the source of wealth and the source of funds of customers and Beneficial Owners identified as PEPs; and

(d) conduct enhanced ongoing monitoring on that relationship.

(2) In relation to domestic PEPs or persons who have been entrusted with a prominent function by an international organisation, in addition to performing the CDD measures required under Section 20, VASPs shall

(a) take reasonable measures to determine whether a customer or the Beneficial Owner is such a person, and

(b) in cases when there is a higher risk business relationship with such a person, adopt the measures in subsections (1)(b) to (d).

23. Transfer of Virtual Assets

(1) For Virtual Asset transfers equal to or greater than [insert *de minimis* threshold]:

(a) originator VASPs shall obtain, and hold required and accurate originator information and required beneficiary information, and submit the required information to the beneficiary VASP or financial institution immediately and securely;

(b) beneficiary VASPs, on transfer, shall obtain and hold required originator information and required and accurate beneficiary information.

(2) A Beneficiary's VASP shall take reasonable measures to identify transfers of Virtual Assets that lack required Originator or Beneficiary information.

(3) A Beneficiary's VASP shall have risk-based policies and procedures for determining when to execute or reject or suspend a transfer of Virtual Asset lacking required Originator or required Beneficiary information and the appropriate follow up action.

(4) The information shall be made available upon the request of the Regulatory Authority or any other competent authority.

(5) For the purposes of this section, Originator information includes:

(a) the name of the Originator; and

(b) the Originator's Virtual Assets account number used to process the transaction or, in the absence of account number, a unique transaction reference number which permits traceability of the transaction; and

(c) the Originator's address, or National ID card, or passport number, or customer identification number, or date and place of birth.

(6) For the purposes of this section, Beneficiary Information includes:

(a) the name of the Beneficiary; and

(b) the Beneficiary's Virtual Asset account number used to process the transaction or a unique transaction reference number which permits traceability of the transaction.

(7) Where several individual Virtual Asset transfers from a single originator are bundled in a batch file for transmission to beneficiaries, the batch file shall contain required and accurate originator information, and full beneficiary information, that is fully traceable within the beneficiary country; and the VASP shall be required to include the originator's account number or unique transaction reference number.

(8) Virtual asset transfers below [insert de minimum threshold] shall always be accompanied by the required originator information in subsection (5) and required beneficiary information in subsection (6).

(9) The information mentioned in subsection (8) does not need to be verified unless there are suspicious circumstances related to money laundering and terrorism financing, in which case information pertaining to the customer should be verified.

(10) The originating VASP shall maintain all originator and beneficiary information collected in accordance with the record keeping requirements in section 21 of this [Act].

(11) The originating VASP shall not execute the Virtual Asset transfer if it does not comply with the above requirements.

Intermediary VASPs

(12) An intermediary VASP shall ensure that all originator and beneficiary information that accompanies a Virtual Asset transfer is retained with it.

(13) Where technical limitations prevent the required originator or beneficiary information accompanying a Virtual Asset transfer from remaining it, the intermediary VASP shall keep a record, for at least five years, of all the information received from the originating VASP or another intermediary VASP.

(14) Intermediary VASPs shall take reasonable measures, which are consistent with straight-through processing, to identify Virtual Asset transfers that lack required originator information or required beneficiary information.

(15) Intermediary VASPs shall be required to have risk-based policies and procedures for determining: (a) when to execute, reject, or suspend a Virtual Asset transfer lacking required originator or required beneficiary information; and (b) the appropriate follow-up action.

(16) VASPs that provide money or value transfer services shall comply with all of the relevant requirements related to money or value transfer services in the countries in which they operate, directly or through their agents.

(17) VASPs that provide money or value transfer services and control both the ordering and the beneficiary side of a Virtual Asset transfer should:

(a) take into account all the information from both the ordering and beneficiary sides in order to determine whether a suspicious transaction report has to be filed.

(b) file a suspicious transaction report in any country affected by the suspicious Virtual Asset transfer and make relevant transaction information available to the Financial Intelligence Unit.

(18) VASPs shall, in the context of processing Virtual Asset transfers, take freezing action and comply with prohibitions from conducting transactions with designated persons and entities, as per obligations set out in the relevant UNSCRs relating to the prevention and suppression of terrorism and terrorist financing, such as UNSCRs 1267 and 1373, and their successor resolutions.

For the consideration of the Commonwealth member countries:

Commonwealth member countries should extend all communication mechanisms, reporting obligations and monitoring requirements that are applied to reporting entities to VASPs to ensure compliance with targeted financial sanctions obligations related to terrorist financing and to proliferation as may be set out in the country's UN Act and/or autonomous sanctions legislation.

(19) For the purposes of counterparty due diligence, and to mitigate sanctions violations, VASPs shall discover the counterparty prior to the transaction and may request the rejection of transactions based on their risk assessment of the counterparty.

(20) VASPs shall ensure they comply with the provisions of the [insert data protection law of the Jurisdiction] and s that customers consent to all inbound and outbound transactions where personally identifiable information of customers is being shared between VASPs.

(21) VASPs shall provide due diligence information on a Person prior to completing transactions, and custodial address verifications prior to each transaction to ensure verification, authentication and due diligence is met.

For the consideration of the Commonwealth member countries:

This provision is added to codify the implementation of the FATF Recommendation 16 that talks about the "**FATF Travel Rule**". In essence, the Travel Rule requires that any transaction that crosses a *de minimus* threshold of the equivalent of USD/EUR 1000 must be accompanied by the personal information of the customer. We recommend that countries adopt the equivalent of this threshold.

Additionally, VASPs must sanction screen the counterparty customer, and perform due diligence on the counterparty VASP.

Sunrise Issue

Notably, the inconsistent adoption of Travel Rule across jurisdictions has led to the "sunrise issue". Here, the Originator and Beneficiary may be located in Countries A and B respectively, and the laws in Country A may require compliance with the Travel Rule by VASPs, but the laws of Country B may not. The key to the effectiveness of the Travel Rule as solution to minimise financial risk is its global adoption and implementation. A standardised approach by all Commonwealth member countries can help achieve this goal.

Further, since countries may adopt the FATF Travel Rule at different times, it is important to ensure compliance when not all parties are subject to the same regulations at the same time. It is also important to address the "sunrise issue" with innovative "historic look back" capability. This feature will allow VASPs to comply retroactively by obtaining transaction information even if it occurred before the counterparty had implemented a Travel Rule solution.

Privacy

It is also important that Travel Rule compliance protects personally identifiable information with

the highest security standards, prioritizing data safety. Robust consent frameworks, data security standards and encryption protocols are not just beneficial but essential to protect data. Secure data transmission channels are equally crucial to safeguard user information from unauthorized access. It will be important to ensure that customers sign off on all deposits and withdrawals to ensure they are aware that their personally identifiable information is being transmitted across jurisdictions and across VASPs. Therefore, the data protection laws of the jurisdiction, especially governing consent and cross border data transfers, will be crucial in this regard.

Way Forward – A standardised, commonwealth wide opportunity

As more countries implement the Travel Rule, the onus will be on VASPs to adopt solutions that adeptly manage detailed customer information exchanges—without slowing down transactions or infringing on user privacy.

It will be important to ensure that challenges like interoperability are considered to achieve effective compliance. VASPs, by collecting and transmitting uniform data points will aid law enforcement and help build standardised open discovery registries.

Open: We recommend that travel rule solutions use open, and publicly verifiable counterparty discovery systems. Global registries of VASPs, across jurisdictions, and the addresses they are requesting to send to, should be publicly available in order to aid law enforcement in travel rule monitoring. Due to the nature of pseudo anonymity that exists between addresses, and their custodial owners, open discovery registries enable verifiable proof that requests are being made between correct counterparties**.** Open systems ensure we have built trust and reliance and mitigate companies controlling critical data pipelines,

Verifiable: Licensing and registration information of VASPs should be publicly visible for all global VASPs to view. This ensures the identity of the jurisdictions VASPs can be cross referenced with the local regulators, and aids both VASPs and law enforcement in cross-jurisdictional coordination, and investigations related to transactions and parties to them.

Secure and Decentralised: To ensure data privacy laws and to ensure against malicious attacks on customer data between VASPs, VASPs must be able to connect with any counterparty VASP immediately and securely using an immutable open directory of all VASPs, before a transaction is executed If these registries are sufficiently decentralised, they can ensure the security of citizens' private data and to prevent malicious actors from having access to 'honeypots' of data. We recommend that solutions strive to use or produce open-source software to maximise trust, participation, and review across a multitude of stakeholders. In order to prevent malicious attacks, a VASPS must be able to send data on a peer-to-peer basis -data should not pass through centralised servers or systems but should only go VASP to VASP.

Global: Unifying the technology requirements at the national level, and across jurisdictions like the commonwealth would enable global travel rule adoption, and a reduction in the issues facing

industry and law enforcement globally in travel rule implementation.

In conclusion, a unified Commonwealth-wide open discovery system (one registry for all VASPs and addresses they try to send Virtual Assets, Fiat Currency, and personally identifiable information to) will be extremely beneficial in this regard. **This could make the Commonwealth the first collective set of countries to universally comply and aid in a global effort to comply with AML/CFT measures.**

24. Reliance on third-parties

(1) Where a VASP relies on a third party to perform the CDD measures set out in section 20 related to customer identification, beneficial owner identification, and understanding the nature of the business, the ultimate responsibility for CDD measures shall remain with the VASP that is relying on the third party and the VASP shall:

(a) obtain immediately the necessary information concerning the elements specified in section 20(2);

(b) take steps to satisfy itself that copies of identification data and other relevant documentation relating to CDD requirements will be made available from the third party upon request without delay;

(c) satisfy itself that the third party is regulated, and supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with all the requirements of this [Act];

(2) For VASPs that rely on a third party that is part of the same group, the requirements of the criteria above may be considered to be met in the following circumstances:

(a) the group applies CDD and record-keeping requirements and programs against money laundering and terrorism financing, in accordance with Part IV;

(b) the implementation of those CDD and record-keeping requirements and AML/CFT programs is supervised at a group level by a competent authority in the relevant jurisdiction; and

(c) any higher country risk is adequately mitigated by the group's AML/CFT policies.

25. Suspicious Transaction Reporting (STR)

(1) If a VASP suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorism financing, it shall report promptly its suspicions to the Financial Intelligence Unit of the [Jurisdiction].

(2) VASPs shall report all suspicious transactions, including attempted transactions, regardless of the amount of the transaction.

For the consideration of the Commonwealth member countries:

The reference to funds or value-based terms, such as "property", "proceeds", "funds", "funds or other assets" and "corresponding value" contained in any financial services legislation or any other enactment relating to money laundering, terrorist financing and proliferation financing shall be construed to include virtual assets with such modifications as may be necessary.

26. Counterparty VASP relationships

(1) In relation to counterparty VASP relationships that involve activities similar to correspondent banking, VASPs shall:

(a) gather sufficient information about a counterparty VASP to understand fully the nature of its business, and to determine from publicly available information the reputation of the VASP and the quality of supervision, including whether it has been subject to a money laundering and terrorism financing investigation or regulatory action.

(b) assess the counterparty VASP's AML/CFT controls.

(c) obtain approval from senior management before establishing new counterparty VASP relationships, and

(d) clearly understand the respective AML/CFT responsibilities of each VASP.

(2) With respect to counterparty VASP relationships like "payable-through accounts", VASPs shall be required to satisfy themselves that the counterparty VASP:

(a) has performed CDD obligations on its customers that have direct access to the accounts of the VASP,

(b) can provide relevant CDD information upon request to the VASP.

(3) VASPs shall not enter, or continue, relationships similar to correspondent banking with shell banks. VASPs must satisfy themselves that their counterparty VASPs do not permit their accounts to be used by shell banks.

For the consideration of the Commonwealth member countries:

FATF also requires VASPs that provide MVTS should be licensed or registered in the [Jurisdiction], should be subject to monitoring for AML/CFT compliance. This may be done either under the ambit of this law, or under the regulatory remit of the country's central bank.

27. High risk countries

VASPs shall apply enhanced due diligence, proportionate to the risks, to business relationships and transactions with Natural Persons and Legal Persons from countries for which this is called for by the FATF.

28. Tipping off and confidentiality

(1) VASPs and their directors, officers and employees shall be protected by law from both criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the Regulatory Authority or such other regulatory body in the [Jurisdiction] responsible for supervision of AML/CFT obligations. This protection should be available even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred.

(2) VASPs and their directors, officers and employees shall not disclose the fact that an STR or related information is being filed with the Regulatory Authority or such other regulatory body in the [Jurisdiction] responsible for supervision of AML/CFT obligations.

29. Internal controls, foreign branches and subsidiaries

(1) Every VASP shall develop and implement procedures for the prevention of activities related to identified risks.

(2) The procedures referred to in subsection (1) shall be:

(a) approved by senior management and be monitored and enhanced, as necessary;

(b) appropriate to the risks identified under section 19 of this [Act]; and

(c) proportionate to the nature and size of the VASP's business, but must at a minimum include:

(i) internal policies, procedures and controls to fulfil the obligations pursuant to this [Act];
(ii) adequate screening procedures to ensure appropriate and high standards when hiring employees;
(iii) on-going training for all directors, officers and employees to maintain awareness of the laws and regulations relating to identified risks, to assist in recognising transactions and actions that may be linked to identified risks, and instruct them in the procedures to be followed in such cases; and

(iv) independent audit arrangements to review and verify compliance with and effectiveness of the measures taken in accordance with this [Act].

(3) All VASPs that are part of a group of entities and that are required to be compliant with this [Act] shall implement group-wide policies and procedures against activities relating to identified risks, addressing all aspects under sections 26(1) and (2), and including policies and procedures for sharing of information within the group for or related to customer due diligence, management of any identified risks and for safeguarding the confidentiality and use or the shared information

(4) The policies and procedures referred to in subsection (3) shall be applied to all branches and majority owned subsidiaries the group.

(5) Any compliance officer who conducts group-level compliance, audit, AML/CFT functions shall have the power to request account and transaction information of customers from branches and subsidiaries as necessary to fulfil their functions.

PART V - INITIAL VIRTUAL ASSET OFFERING

30. Issuers of Initial Virtual Asset Offerings

(1) A Natural Person shall not offer for issue a Virtual Asset to the public as a business in the [Jurisdiction].

(2) A Legal Person shall only offer for issue a Virtual Asset to the public in the [Jurisdiction] in the manner set out under this [Act].

31. Obligations of Issuers of Initial Virtual Asset Offerings

(1) A Legal Person shall not offer for issue a Virtual Asset to the public unless the Person:

(a) has made publicly available online, and easily accessible, a White paper that:

(i) describes the name of the Legal Person responsible for issue of the Virtual Assets, including its country of registration and contact information;

(ii) name(s) of the Beneficial Owners of the Legal Person;

(iii) names the Legal Person responsible for the content of the White paper, including its country of registration and contact information;

(iv) is drafted in a fair, clear, concise and effective manner;

(v) includes the date on which the White paper was published;

(vi) describes all the information about the Virtual Asset that a holder of the Virtual Asset would reasonably be expected to need to know, including any rights or obligations attached to the Virtual Asset;

(vii) describes the types of Persons that the Virtual Asset would be appropriate to, and the types of Persons that the Virtual Asset would not be appropriate to;

(viii) describes in a balanced manner, the risks and benefits of the Virtual Asset and its uses;

(ix) includes a prominent risk warning about the possibility of the Virtual Asset reducing in value to zero, and about situations where the Virtual Asset will not be liquid;

(x) discloses the types of venues where the Virtual Asset will be available for secondary market trading;

(xi) discloses all applicable fees and costs associated with acquiring and holding the Virtual Asset, when and how they are calculated, and when and to whom they are paid;

(xii) includes the full legal names, contact details and registration status of any independent third-party assurance providers who have reviewed the contents of the White paper and the extent of any limitations of their review. If no independent assurance provider has undertaken assurance, the white paper must disclose a prominent warning that no assurances have been undertaken;

(xiii) includes information about any adverse impacts that the technology underlying the Virtual Asset has on the environment;

(xiv) includes information about who is the legal owner of the virtual assets before they are issued, and how legal ownership changes when the issue takes place;

(xv) includes a translated version of the White paper, in each jurisdiction where subscriptions of the Virtual Asset are available;

For the consideration of the Commonwealth member countries:

VASPs should also be responsible for ensuring White papers are robust and should not offer liquidity/secondary market services for Virtual Assets with being satisfied with the contents of the White paper.

Notably, a VASP, if offering for sale a Virtual Asset, should conduct due diligence on the Virtual Asset and its Issuer, taking into account the requirements of a White paper set out in the section titled "Initial Virtual Asset Offerings".

(b) notifies the Regulatory Authority of its intention to make the Virtual Asset available to the public, where the total amount of Virtual Assets made available in this [Jurisdiction] exceeds [insert threshold amount].

For the consideration of the Commonwealth member countries:

Commonwealth member countries may require Issuers to notify the Regulatory Authority where the total amount of Virtual Assets made available by the Issuer exceeds a certain threshold. The threshold may be decided by Commonwealth member countries based on their own economic dynamics.

(2) An Issuer shall:

(a) provide its services honestly and fairly;

(b) not communicate anything in connection with the sale or issue of a Virtual Asset that is false, misleading or deceptive;

(c) not receive or pay any commission or fee that is not fully and prominently disclosed;

(d) not make available a Virtual Asset, if the Virtual Asset relates to goods or services that are not yet operational within a period of 12 months from when the sale or issue is first made;

(e) not promote the Virtual Asset before the White paper is made publicly available;

(f) on an ongoing basis (at least monthly), publicly disclose the number of Virtual Assets currently in circulation;

(g) manage conflicts of interest related to the offer of issue of Virtual Assets;

(h) comply with the same market conduct obligations (relating to misuse of non-public information, or market manipulation, or related market conduct rules) as if the Virtual Assets were tradeable securities on a licensed market.

For the consideration of the Commonwealth Members:

Regulatory Authorities may choose to exempt certain Issues - say, where there are less than 20 issues or sales within a 12-month period, and no more than [insert threshold amount] is raised.

Regulatory Authorities may also choose to create a dual-regulatory obligation - imposing stricter standards when the Initial Virtual Asset Offering is available to retail customers vs institutional customers.

PART VI - SUPERVISION AND ENFORCEMENT

32. Investigation and examination

(1) All Persons acting as VASPs or Issuers of Initial Virtual Asset Offering, shall be:

(a) subject to investigation and/or examination by the Regulatory Authority at any time or in any way deemed necessary by the Regulatory Authority for the purposes of exercising its powers, performing its functions, or fulfilling its objectives under this [Act];

(2) required to co-operate with the Regulatory Authority during any investigation and/or examination;

(3) required to provide the Regulatory Authority with any information requested by the Regulatory Authority to facilitate any investigation and/or examination.

33. Enforcement

(1) The Regulatory Authority may, in its sole and absolute discretion, take enforcement action against any Person who:

(a) violates any provision of this [Act];

(b) recklessly or negligently makes any representation under this [Act] that they know to be false or misleading; or

(c) obstructs the Regulatory Authority or any person authorised by the Regulatory Authority in the performance of duties under this [Act].

(2) The enforcement action that the Regulatory Authority may take includes but is not limited to:

(a) issuing written reprimands;

(b) issuing enforcement notices requiring non-compliance to be rectified within a specified period of time;

(c) suspending or revoking a license;

(d) requiring a Person to cease any activity or activities undertaken by it or indefinite period of time;

(e) limiting or revising the scope of any Virtual Assets or VASP activities under a licence;

(f) imposing such fines as determined by the Regulatory Authority from time to time;

(g) undertaking additional supervision, monitoring or reporting requirements; and

(h) taking any other enforcement action determined by the Regulatory Authority.

(3) If an offence under this [Act]; is committed by a Legal Person, the Director of the Legal Person who authorised, permitted or acquiesced in the commission of the offence also commits the said offence and is liable to a fine and/or imprisonment.

For the consideration of the Commonwealth member countries:

There may be a range of proportionate and dissuasive sanctions, whether criminal, civil or administrative, available to deal with VASPs that fail to comply with AML/CFT requirements. FATF recommends that such sanctions should be applicable not only to VASPs, but also to their directors and senior management.

(4) The Regulatory Authority, when determining the appropriate enforcement action, shall consider the following factors:

(a) the nature, seriousness and impact of the violation;

(b) the conduct of the Person after the violation and throughout any investigation or examination by the Regulatory Authority;

(c) the previous disciplinary record and compliance history of the Person;

(d) the interpretation and application of the Regulatory Authority published materials including Guidance, industry codes and other such materials as may be published from time to time; and

(e) any action taken by the Regulatory Authority or by other domestic or international regulatory bodies in similar cases.

PART VII - MISCELLANEOUS

34. Appeals

(1) A Person may appeal to the [Appellate Body] against a decision of the Regulatory Authority to take enforcement action.

(2) The appeal shall be made within [X] days of the Regulatory Authority's decision.

(3) In determining an appeal, the [Appellate Body] may:

(a) confirm, vary or revoke the decision of the Regulatory Authority; and

(b) make further orders as it considers appropriate.

For the consideration of the Commonwealth member countries:

Commonwealth member countries may determine the appellate process and timelines based on their marker readiness and applicable judicial systems.

35. Regulations

The [Minister / Regulatory Authority] may make such [delegated legislation] as she/he thinks fit for the purposes of this Act.

For the consideration of the Commonwealth member countries:

Commonwealth member countries may consider inserting savings and transitional provisions as well as consequential amendments, as necessary.

36. Commencement

This [Act] comes into force on the day on which it is published in the official Gazette of the [Jurisdiction].

Way Forward

Delegated Legislation

Commonwealth member countries may, depending upon their market maturity and regulatory readiness, customise this Model Law for the peculiar dynamics of their economies. This may be done by way of extensive and delegated legislation, such as implementing regulations, guidance, circulars, rules, FAQs, among others. For example, the licensing application procedure, relevant timelines (and clock-stops, if any), administrative fees, offences and penalties for non-compliance may be detailed in delegated legislation.

Follow on Amendments

While this Model Law may only focus on Virtual Assets, there may be a need to amend other applicable laws to align them with the respective Virtual Assets laws. This may include, inter alia, amendments to the applicable AML/CFT laws.

Ecosystem Considerations

Notably, world over, authorities and multilateral bodies are discussing the definitional challenges related to the crypto economy. A key component of this debate is the definition of Virtual Assets. For example, FATF defines Virtual Assets as digital representation of value that can be digitally traded, transferred or used for payment. Notably, it does not include digital representation of Fiat Currencies. Other components of the crypto ecosystem include Decentralised Finance or DeFi, Central Bank Digital Currencies, Decentralised Autonomous Organisations, Non-Fungible Tokens, among others. Regulatory frameworks, depending upon the market dynamics of each Commonwealth member country, could potentially factor in the nuances of each of these technologies, and anticipate regulatory changes relating to them.

Sandbox

The member countries of the Commonwealth may, by way of delegated legislation or regulatory initiatives, set up regulatory sandboxes and accelerator programmes to provide a secure testing environment to these emerging technologies. This can ensure that these technologies are not unveiled to the world before end-to-end customer protection is ensured, and comprehensive laws have been put in place. Commonwealth member countries may consider setting up cross border sandboxes, and even sharing their learnings from sandboxing regimes by way of MoUs.

Other Technologies

In a similar vein, the rapid advancement of AI technologies requires a dedicated legislative approach. As we witness the transformative potential of AI across various sectors, there is a growing need to establish comprehensive AI laws and regulations. These regulations could encompass issues like overlap of AI and blockchain technologies, AI and data privacy, AI and algorithmic accountability, and ethical AI development. Addressing these aspects within the framework of AI laws will be essential in shaping a responsible and innovative future for AI technologies in the Commonwealth countries.

The Commonwealth