TURKS AND CAICOS ISLANDS

VIRTUAL ASSETS BUSINESS BILL 2026

ARRANGEMENT OF CLAUSES

PART IX

STABLECOINS

PART X

CUSTOMER AND USER PROTECTION

PART XI

SUPERVISION

PART XII

ENFORCEMENT AND APPEALS

PART XIII

MISCELLANEOUS

TURKS AND CAICOS ISLANDS
Act No. [X] of 2026

AN ACT to provide for the regulation, licensing and supervision of virtual asset service providers; to make provision for measures to combat money laundering, terrorist financing and proliferation financing in relation to virtual assets; to provide for initial virtual asset offerings; to regulate the issuance of stablecoins; and for connected purposes.

ENACTED by the Legislature of the Turks and Caicos Islands.

PART I

PRELIMINARY

Short title and commencement

1. (1) This Act may be cited as the Virtual Assets Business Act 2026.

(2) This Act comes into force on such date as the Governor may, by Notice published in the Gazette, appoint.

(3) Different dates may be appointed for different provisions of this Act.

Interpretation

2. (1) In this Act, unless the context otherwise requires—

"AML/CFT/CPF" requirements means all anti-money laundering, counter-terrorist financing and counter-proliferation financing obligations applicable in the Turks and Caicos Islands under any Act, subsidiary legislation, code of practice directive or guidance issued by a competent authority (together, referred to as the "AML legislation";

"authorisation" means a licence or other approval granted under this Act and includes any conditions attached to it;

"authorised person" means any person authorised by the Commission for the purposes of this Act;

"beneficial owner" has the meaning given in the Anti-Money Laundering and Prevention of Terrorist Financing Regulations;

"blockchain" means a type of distributed ledger, consisting of a growing list of records, called blocks, that are securely linked together using cryptographic techniques, wherein each block contains a timestamp and a reference to the previous block, thereby forming a verifiable and immutable chain of information;

"Commission" means the Turks and Caicos Islands Financial Services Commission established under the Financial Services

Commission Act, 2001 and preserved and continued under the Financial Services Commission Act 2007; (or, the "FSCA");

"compensation fund" means a fund designed to reimburse customers in the event of the VASP's insolvency or fraud;

"competent authority" means the Commission as designated in Section 5;

"compliance officer" has the same meaning as provided in Section 31(2) of the FSCA;

"Court" means the Supreme Court of the Islands;

"controller" means a person who, alone or with others, exercises control over a person, whether directly or indirectly, including through ownership of voting rights or by any other means;

"custody" includes safeguarding or administering a virtual asset or the instruments enabling control over a virtual asset (including private keys), on behalf of another person;

"customer" includes a client, user or counterparty of a VASP;

"cybersecurity" means the measures, controls and practices used to protect information systems, networks and data from unauthorised access, misuse, disruption, loss or other cyber threats;

"decentralised" refers to any governance, administrative, financial, or technological arrangement in which authority, control, or decision making power is dispersed among multiple actors such that no single entity retains exclusive or dominant control-making power is dispersed among multiple actors such that no single entity retains exclusive or dominant control;

"director", "chief executive officer" or other prescribed senior officer etc. has the same meaning as referred to under the AML/CTF/CPF requirements;

"distributed ledger technology" or "DLT" means a technological infrastructure and protocols that allow the decentralised recording, sharing, and synchronisation of data across multiple nodes or participants in a network, without the need for a centralised data storage or administration;.

"document" has the same meaning as defined in the Companies Act;

"fiat currency" means banknote or coin that is in circulation as a medium of exchange;

"financial business" has the meaning given to that term in the Banking Act);

"fit and proper" has the meaning assigned to the term in the AML requirements;

"initial virtual asset offering (or virtual asset offering)" means an offer to the public or a section of the public to purchase, subscribe for, or otherwise acquire a virtual asset, where the offer is made by or on behalf of an issuer to raise funds or other value;

"intermediary VASP" is an entity acting as a middleman between two other VASPs to facilitate, settle, or manage the transfer of virtual assets;

"interoperability" means the ability for systems, including blockchains, to interact and transact seamlessly;

"issuer" means a person who issues virtual assets as a business;

"licence" means a licence or an authorisation issued or granted under a regulatory Act and under Part 3 of this Act and includes any conditions attached to it and "licensee" and "licensed" shall be construed accordingly;

"minimum criteria" means the minimum criteria for licensing specified in Schedules 1 and 2;

"Minister" means the Minister responsible for finance or such other Minister as may be assigned responsibility for this Act;

"Mutual Funds Act" means the Mutual Funds Act;

"Money laundering Compliance Officer" or "MLCO" means the person appointed by a financial business under regulation 21 of the AML/CFT Regulations;

"Money Laundering Reporting Officer" or "MLRO" means the person appointed by a financial business under regulation 22 of the AML/CFT Regulations;

"natural person" means an individual who conducts virtual asset activities for a legal person;

"originator", with respect to a transfer of a 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;

"person" includes any natural person, legal person, trust, partnership, unincorporated association, or other body, entity, or arrangement—whether or not possessing separate legal personality or legal capacity under applicable law;

"ordinarily resident", shall be construed in accordance with Section 6 of the Companies Act;

"POCA" means the Proceeds of Crime Act;

"qualified person" means a person appointed pursuant to Section 36 of the Financial Services Commission Act;

"registered agent" or "agent" means a person appointed as a registered agent under the Companies Act;

"Registrar" means the Registrar of Companies appointed under Section 289 of the Companies Act and includes any Deputy or Assistant Registrar of Companies;

"regulatory impact assessment" means an analysis that evaluates the effect of new regulation on stakeholders and the economy yield;

"regulatory sandbox" means a controlled, time-limited regulatory environment established and administered by the Commission that permits the live testing of innovative virtual asset activities, products, services, or business models subject to defined limits, conditions, safeguards and supervisory oversight, where the appropriate regulatory treatment is uncertain or requires empirical testing;

"segregated account" means a custodial or trust account in which customer funds are held separately from the issuer's own assets and cannot be commingled or used for proprietary purposes;

"smart contract" means a self-executing contract with the terms of the agreement directly written into code and thereby manage the issuance, redemption and transactions of virtual assets;

"smart contract custom software code" means the programming code that defines the behavior and rules of the smart contract, and which specifies the conditions under which virtual assets may be issued, transferred or redeemed;

"the Islands" means the Turks and Caicos Islands;

"virtual asset" has the meaning given in subsection (2);

"virtual asset activities (or regulated activities)" has the meaning given in Section 15;

"virtual asset business" has the meaning given in Section 16 and is a "regulated business" under POCA for which a regulatory licence is required;

"virtual asset service provider" or "VASP" means a person who, as a business, conducts one or more virtual asset activities for or on behalf of another person under this Act and designated as a "financial business" for AML/CFT/CPF purposes;

"wallet" means a software program that stores private and public keys and interacts with distributed ledger technology to enable users to send, receive and monitor their digital assets;

"White Paper" means a document prepared by the issuer that meets the requirements of a White Paper as prescribed in Section 43 and Schedule 5.

(2) "virtual asset" means 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 digital representations of fiat currency, securities or other financial assets already covered by an existing law, to the extent so covered;

(3) For the avoidance of doubt, this Act does not apply to the following "virtual assets"—

(a) digital representations of value or rights that operate within a closed ecosystem of the VASP, including those—

(i) non-transferable outside a closed ecosystem;

(ii) non-exchangeable with real-world goods, services, discounts and 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 Islands;

(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 Commission.

(4) The Commission may, by notice published in the Gazette, issue guidance on the interpretation of terms used in this Act.

Scope and application

3. (1) For the purposes of this Act, a person carries on virtual asset business if the person—

(a) is incorporated or registered in accordance with the Companies Act, ordinarily resident in or has a place of business in the Islands in connection with virtual assets activities; or

(b) carries on, or holds out as carrying on, any virtual asset activities as a business in or from within the Islands.

(2) A person carries on virtual asset business in or from within the Islands if the person—

(a) conducts the virtual asset activities from an establishment in the Islands;

(b) provides the activity to persons in the Islands as part of a business offering;

(c) uses digital representations of fiat currency issued by a government, central bank or monetary authority located in the Islands to conduct the activity; or

(d) markets or promotes the activity to persons in the Islands in a manner that indicates an intention to provide such activity to persons in the Islands.

Relationship with other laws

4. (1) Where a virtual asset, product or activity is regulated under another law, including the Investment Dealers (Licensing) Act or the Mutual Funds Act (as applicable), the Banking Act, the Insurance Act or any law relating to payment systems, the Commission shall coordinate with the relevant competent authority and may determine whether the activity is to be regulated under this Act, that other law, or both.

(2) Without limiting subsection (1), a virtual asset that constitutes a security, derivative or other regulated instrument under the Investment Dealers (Licensing) Act or the Mutual Funds Act (as applicable) shall be treated as such and this Act shall not be interpreted as exempting the virtual asset or any related activity from applicable securities or investment law requirements.

(3) To the extent possible, the provisions of this Act shall be construed consistently with the provisions of the Companies Act and any other law governing the incorporation, registration, administration, insolvency, winding-up or dissolution of persons carrying on business in or from within the Islands;

(4) where there is an inconsistency between this Act and the Companies Act or any other law referred to in subsection (3), this Act shall prevail to the extent of the inconsistency in relation to the regulation, licensing, supervision and enforcement of virtual asset business.

(5) Nothing in this Act limits the application of the AML/CFT/CPF requirements or any other law relating to anti-money laundering regulations, sanctions, consumer protection, financial services, companies or insolvency; and

(6) The Commission may pursuant to the power granted under Section 40 of the Financial Services Commission Act and under this Act, on application or on its own initiative, grant an exemption from specified requirements of this Act, subject to conditions, where the Commission is satisfied that the exemption is consistent with the object of this Act and does not materially increase risk.

PART II

FINANCIAL SERVICES COMMISSION AS COMPETENT AUTHORITY

Designation of competent authority

5. (1) The Commission is designated as the competent authority for the regulation, licensing, supervision and enforcement of compliance of VASPs and virtual asset activities in or from within the Islands under this Act.

(2) The FSCA and subsidiary legislation and Code made under that Act are incorporated by reference in this Act, as applicable.

Objectives of the Commission

6. In performing its functions under this Act, the objectives of the Commission are to—

(a) protect the integrity and reputation of the Islands as a financial services jurisdiction;

(b) safeguard consumers and market participants;

(c) reduce systemic, prudential and operational risks arising from virtual asset activities;

(d) promote compliance with AML/CFT/CPF requirements and sanctions obligations; and

(e) support responsible innovation consistent with international standards.

Functions of the Commission

7. The functions of the Commission under this Act, the FSCA and any other Act, include—

(a) receiving, assessing and determining applications for licences and approvals and conditions applicable to any such licence;

(b) setting prudential, conduct, governance, technology and AML/CFT/CPF requirements for VASPs;

(c) identify, assess and monitor risks arising from virtual asset activities and the activities of VASPs, and apply a risk-based approach to mitigating such risks;

(d) supervising compliance through off-site monitoring and on-site inspections;

(e) maintaining registers and publishing information for transparency;

(f) taking enforcement action, including administrative penalties and licence action;

(g) cooperating and exchanging information with domestic and foreign authorities; and

(h) promoting public awareness and issuing consumer advisories.

Powers of the Commission

8. (1) This Section confers on the Commission its core supervisory, investigative, rule-making and enforcement-triggering powers, which are operationalised through Part 11 and enforced through Part 12.

(2) The Commission may do all things necessary for, or reasonable ancillary or incidental to the carrying out of its duties and the exercise of its powers under this or any other Act, including power to—

(a) grant, refuse, suspend, vary, revoke or conditions applicable to any licence;

(b) require information, documents, data and explanations from any person;

(c) require independent assurance, audits, attestations and expert reports;

(d) conduct investigations and examinations and enter premises in accordance with Section 92*;*

(e) issue directions, codes, rules, notices and guidance to VASPs or classes of persons in accordance with Section 93;

(f) impose administrative penalties under Section 94; and

(g) apply to the Court for orders under Sections 95 to 97.

(3) The Commission may publish, in such manner as it considers appropriate, guidance, codes and regulatory standards to give effect to this Act.

(4) A code, rule or standard issued under subsection (2) may make different provision for different classes of VASP, activities, products or risks, and may include transitional provisions.

(5) The Commission must—

(a) recognise, approve or prescribe criteria for VASPs, including persons providing smart contract audits, cybersecurity audits, reserve attestation, custody technology assurance and blockchain analytics services; and

(b) any other related services and may require a VASP to obtain services from an independent professional body, recognised and approved by the Commission.

(6) The Commission may do all things necessary or incidental to the exercise of its functions and powers under this Act.

Delegation and use of qualified persons or agents

9. (1) Without prejudice to Section 15 of the FSCA, the Commission must, in writing, delegate any of its functions or powers under this Act to a member, officer, employee or committee of the Commission, subject to such limitations or conditions as the Commission may specify.

(2) The Commission may appoint suitably qualified persons to assist it, including as inspectors, investigators or experts, and may require a VASP to bear the reasonable cost of any special review where the Commission considers it necessary for supervisory purposes.

Co-operation and information sharing

10. (1) Without prejudice to Section 23 of the FSCA, the Commission shall cooperate and exchange information with—

(a) the Anti-Money Laundering Committee and the Financial Intelligence Agency;

(b) law enforcement agencies and prosecuting authorities;

(c) overseas regulators and law enforcement agencies;

(d) any other body responsible for financial stability, consumer protection or market integrity;

(e) domestic and foreign tax authorities; and

(f) international standard-setting bodies.

(2) The Commission may enter into memoranda of understanding or other arrangements to facilitate information exchange and supervisory cooperation, in relation to virtual asset activities that operate across borders.

(3) Information obtained under this Act may be disclosed where disclosure is necessary for—

(a) the performance of functions under this Act or related laws; or

(b) the prevention, investigation or prosecution of an offence; or

(c) compliance with a lawful request from a competent authority, subject to confidentiality safeguards.

Confidentiality and protection of information

11. (1) A person who, in the course of performing functions under this Act, obtains confidential information shall not disclose that information except as permitted by this Act or any other law.

(2) Subsection (1) does not prevent disclosure of information—

(a) in aggregated or anonymised form;

(b) with the consent of the person to whom the information relates; or

(c) where required by a court order or lawful process.

(3) A person may disclose to the Commission information relating to a suspected contravention of this Act, any regulations, rules or authorisation conditions, or to risks to customer assets or market integrity.

(4) A disclosure under subsection (3) is a protected disclosure if made in good faith and on reasonable grounds.

(5) No civil, criminal or disciplinary proceedings lie against a person for making a protected disclosure, and the person does not breach any duty of confidentiality by doing so.

(6) The Commission shall take reasonable steps to protect the identity of a person making a protected disclosure, subject to lawful process.

(7) A person who victimises another person because that other person has made, or proposes to make, a protected disclosure commits an offence and is liable on conviction to the penalties prescribed in Section 99.

(8) A person who contravenes this Section commits an offence is liable on conviction to penalties prescribed in Section 99.

PART III

LICENSING OF VIRTUAL ASSETS BUSINESS

Prohibition on carrying on VASP business without licence

12. (1) Subject to Sections 14 to 16, a person, authorised person or agent on behalf of a legal entity shall not carry on or purport to carry on virtual asset business in or from within the Islands unless that person holds a valid licence granted under one of the license classes specified in Schedule 3.

(2) The Commission may license a person to carry on one or more of the virtual asset activities as a business as follows—

(a) issuing, selling or redeeming virtual coins, tokens or any other form of virtual assets;

(b) operating as a payment VASP utilising virtual assets which includes the provision of services for the transfer of funds;

(c) operating as a virtual asset exchange;

(d) carrying on digital asset trust services;

(e) providing custodial wallet services;

(f) operating as a virtual asset derivative exchange provider;

(g) operating as a VASP;

(h) operating as a virtual asset lending or virtual asset repurchase transactions legal entity;

(i) any other activities related to virtual assets that the Commission may from time to time prescribe in regulations.

(3) No person carrying on business in or from within the Islands shall use any name which indicates or may reasonably be understood to indicate (whether in English or in any other language) that it is carrying on virtual asset business unless it is a licensed undertaking under this Act.

(4) For the purposes of this Section, a person is regarded as acting "as a business" where the person conducts any activity specified in Section 15 for commercial benefit, gain or regular course of trade.

(5) A number of factors shall be taken into account in determining whether a person is carrying out an activity as a business, including—

(a) the nature of the particular regulated activity that is carried on;

(b) the existence of a commercial element;

(c) the act of holding oneself to be willing and able to engage in the regulated activity;

(d) the act of soliciting clients to offer them services falling under the regulated activity;

(e) the scale of the activity;

(f) the proportion which the activity bears to other activities carried on by the person but which are not regulated; and

(g) the degree of continuity of the above.

(5) The Commission may by order amend subsection (2) by adding new provisions, or by amending, suspending or deleting any of the virtual asset activities set out thereunder.

(6) Any person using a name in contravention of subsection (1) commits an offence and is liable on conviction to the penalties prescribed in Section 99.

(7) In accordance with section 104 an order made under this Section shall be laid before Parliament.

Virtual asset activities

13. (1) For the purposes of this Section, a person shall not carry on or purport to conduct any virtual asset activities as a business unless that person is in compliance with Section 13 and any conditions imposed by the Commission.

(2) For the purposes of this Act, "virtual asset activities" include the following activities, whether conducted for fiat currency, virtual assets, or any other form of value—

(a) exchange between virtual assets and fiat currencies;

(b) exchange between one or more virtual assets;

(c) transfer of virtual assets;

(d) safekeeping or administration of virtual assets or instruments enabling control over virtual assets (including custody);

(e) participation in and provision of financial services related to an issuer's offer or sale of a virtual asset;

(f) operation of a virtual asset trading platform or marketplace;

(g) any other activity prescribed in regulations.

Carrying on virtual asset business

14. (1) For the purposes of this Section, a person carries on virtual asset business if they engage in any activity as referred to in Section 15 as a VASP or authorised person or agent acting on behalf of a VASP.

(2) For the purposes of this Act, a person carrying on virtual asset activities as a VASP, if—

(a) any person actively markets, whether domestically or internationally, to the public that such person carries on, or purports to carry on, such activity; and

(b) the activity, if carried on within a regulated financial framework, would constitute a virtual asset activity.

(3) Subsection (1) applies in relation to a VASP regardless of—

(a) whether the carrying on, or purported carrying on, of an activity mentioned in subsection (2)(a) is actively marketed by the VASP or another person on behalf of the VASP; and

(b) whether the activity mentioned in section 16(2)(a) is carried on or not.

(4) The Commission may, after consulting relevant financial authorities, specify an activity for the purposes of this Act.

(5) In exercising a power to specify an activity under subsection (4), the Commission must, in addition to any other matters that the Commission considers relevant, have regard to—

(a) whether the activity is, or is likely to become, material to the monetary or financial stability of the Islands;

(b) whether the activity is, or is likely to become, material to the functioning of the Islands as a financial services jurisdiction; and

(c) the matters of significant public interest, including—

(i) the protection of customers, investors, or end-users of stablecoin systems;

(ii) the prevention of financial crime, including money laundering, terrorist financing, and proliferation financing;

(iii) systemic risks arising from market concentration, technological failure, or governance weaknesses;

(iv) the promotion of competition, innovation, and financial inclusion; and

(v) the upholding of public trust and confidence in the digital financial system.

(6) For the purposes of subsection (5)(a), an activity is or is likely to become material to monetary or financial stability, if the occurrence of any significant disruption to the carrying on of the activity is likely to adversely affect financial system stability.

(7) For the purposes of subsection (5)(b), an activity is or is likely to become material to the functioning of a financial services jurisdiction, if the occurrence of any significant disruption to the carrying on of the activity is likely to—

(a) adversely affect the role of the Islands as a financial services jurisdiction; or

(b) cause systemic disruption to the financial system.

(8) For the purposes of subsection (5)(c), the following matters are to be regarded as matters of significant public interest—

(a) whether the occurrence of any significant disruption to the carrying on of the activity is likely to adversely affect the public's confidence in the financial system; and

(b) whether the occurrence of any significant disruption to the carrying on of the activity is likely to adversely affect day-to-day commercial activities.

(9) For the purposes of this Section, "conduct", "directed at" or "carrying on" includes the active provision or facilitation of a virtual asset activity.

Excluded activities

15. This Act does not apply to—

(a) a person who provides goods or services in exchange for virtual assets solely as payment for such goods or services and not as a business of virtual asset activities;

(b) a person who develops or sells software or hardware, including non-custodial wallets, solely as a technology provider and not as a business of virtual asset activities;

(c) miners, validators, node operators or other persons who provide ancillary infrastructure services, to the extent they do not otherwise carry on business as a VASP; and

(d) such other persons or activities as may be as prescribed by Regulations.

Exemption Order

16. (1) Section 16 does not apply to any person exempted by or under an exemption order issued in terms of this Section.

(2) The Commission may issue an exemption order, which may provide for—

(a) a specified person; or

(b) persons falling within a specified class, to be exempt from the requirement of Section 12.

(3) An exemption order may provide for an exemption to have effect—

(a) in respect of all virtual asset activities under Section 13;

(b) only in respect of one or more of such virtual asset activities; or

(c) in respect of specified circumstances.

(4) An exemption order may be subject to conditions.

(5) An exemption order made under this Section may specify activities that do not constitute virtual asset business for the purposes of Section 13(1).

(6) In subsection (3)(c), "specified" means specified by the exemption order.

(7)An order made under this Section shall be laid before Parliament and shall be subject to the negative resolution procedure.

Cross-border services; recognition of overseas VASPs

17. (1) No person incorporated or established outside the Islands shall provide virtual asset activities in or from within the Islands unless—

(a) the person is licensed under this Act; or

(b) the person is registered by the Commission under a recognition framework as prescribed in Schedule 12, any other regulation in the Islands, or under any other foreign legal or regulatory regimes.

(2) The Commission may recognise or register an overseas VASP where it is satisfied that—

(a) the VASP is subject to effective supervision in a jurisdiction with equivalent standards;

(b) adequate cooperation and information-sharing arrangements are in place; and

(c) the VASP appoints authorised persons in the Islands and submits to the jurisdiction of the courts.

(3) The Commission may impose conditions or restrictions on any recognised or registered overseas VASP.

(4) A person who contravenes this Section commits an offence and is liable on conviction to penalties prescribed in Section 99.

(5) The Commission may apply to the Court for an injunction or other order under Section 95 restraining a person from contravening this Section.

Application for a VASP licence

18. (1) An application for a VASP licence shall be filed with the Commission in the form and accompanied by such information and such fee as may be as prescribed by Regulations.

(2) An application shall include, at a minimum—

(a) information specified in Schedule 1; and

(b) any other information required by the Commission.

(3) An application shall state the class of VASP licence required, as prescribed in Schedule 3.

(4) The Commission may require the applicant to provide additional information, clarifications or documents within a specified period.

(5) The Commission may —

(a) establish such additional classes and categories of VASP licences as it considers appropriate, having regard to innovation in virtual asset activities;

(b) The Commission may require a person to hold more than one class of licence where the person conducts multiple activities;

(c) The Commission may issue classification guidance and may require a person to obtain independent legal advice or a written classification opinion as part of an application or as a continuing condition of a licence;

(d) The Commission may prescribe higher or activity-specific requirements or licence conditions (including for stablecoin arrangements and tokenisation of real-world asset activities), as may be determined from time to time; and

(e) The Commission may publish guidance on virtual asset classification and categories and may consult with other competent authorities.

Assessment of applications; fit and proper

19. (1) The Commission shall assess an application having regard to the objects of this Act and any other Act, without limitation, and consider among other things, whether—

(a) the applicant and its controllers, beneficial owners, directors and senior management are fit and proper;

(b) the applicant has adequate financial resources and capital for the nature and scale of its business;

(c) the applicant has appropriate governance, risk management, internal controls and compliance arrangements;

(d) the applicant has adequate technology systems, cybersecurity, operational resilience and incident management capabilities;

(e) the applicant can comply with AML/CFT/CPF requirements and sanctions obligations, including the travel rule;

(f) the applicant has appropriate arrangements for safeguarding customer assets and funds where relevant;

(g) the applicant has a physical presence, staffing, and operational capability appropriate to its business model in the TCI, including to support effective supervision.

(2) The Commission may interview persons, obtain references, and consult domestic or foreign authorities as part of its assessment.

(3) The Commission may within a reasonable period of time—

(a) accept the application and designate the applicant as a VASP; or refuse an application where it is not satisfied of any matter in subsection (1);

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

(4) The Commission 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 Commission 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 Commission may require;

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

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

(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 VASP 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 Commission;

(h) if the services to be provided by the applicant will be provided in a manner that will or is likely to bring the Islands 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 Commission may deem fit.

(5) A licensee shall ensure that it, and each of its directors, senior officers, beneficial owners and key function holders, are and remain fit and proper persons at all times.

Grant or refusal; conditions

20. (1) Where the Commission grants a licence, it shall issue the licence in writing and may impose such conditions as it considers necessary or desirable, including conditions relating to—

(a) scope of activities, customers and jurisdictions served;

(b) capital, liquidity, insurance or other financial requirements;

(c) safeguarding and custody arrangements;

(d) reporting, audits and independent assurance;

(e) technology standards and incident reporting;

(f) AML/CFT/CPF controls, including enhanced measures for higher-risk activities; and

(g) outsourcing and third-party arrangements.

(2) Where the Commission refuses an application, it shall give written notice of the refusal and the reasons for it, subject to any confidentiality or law enforcement considerations.

(3) A person aggrieved by a decision of the Commission under this Section may, within such period as may be prescribed, appeal against that decision in accordance with Section 100.

Term, renewal, assignment and fees

21. (1) A VASP licence is valid for such period as may be prescribed, and may be renewed in accordance with the prescribed procedure.

(2) An application for renewal shall be made not less than the prescribed period before expiry and shall be accompanied by the prescribed fee.

(3) A VASP may not assign or transfer a licence. Any purported assignment or transfer of a VASP licence is void and of no effect.

(4) The Commission may impose annual fees and supervisory levies, including risk-based levies, as may be prescribed.

(5) Subject to Section 103, the fees payable under this Section, including the periods within which such fees are to be paid, shall be prescribed by the Commission.

(6) A person who fails to comply with subsections (2) and (3) commits an offence and is liable on conviction to penalties prescribed in Section 99.

Public register and display of licence

22. (1) The Commission shall establish and maintain a register of all licensed VASPs and authorised persons, including VASPs and authorised persons under the regulatory sandbox.

(2) As soon as practicable after a licence has been issued to the applicant, the Commission shall include in the register the following details—

(a) name of the VASP;

(b) the name and registered address of the VASP;

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

(d) the licence number and class;

(e) any conditions imposed; and

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

(3) The Commission may publish the register or a portion of it in such manner as it considers appropriate.

(4) Once registered, a VASP shall prominently display its licence on or at its principal place of business in the Islands (if any) and all other places where it conducts virtual asset activities, including on its website and customer-facing communications, or in such manner as the Commission may prescribe.

Change of control and key persons

23. (1) A VASP shall not, without the prior written approval of the Commission—

(a) effect a change of controller or beneficial owner;

(b) appoint or remove a director, chief executive officer or other prescribed senior officer; or

(c) materially change its business model, activities, products, markets, or custody arrangements.

(2) Without prejudice to the foregoing, any change in the directors, senior officers or auditor of a licensed VASP shall be notified to the Commission within fourteen (14) days of such change and details of the newly appointed directors, senior officers or auditor, with, in the case of an auditor, the auditor's written consent to act, shall be given with such notification.

(3) An application for approval under subsection (1) shall be filed in the prescribed form and manner supported by such information as the Commission may require.

(4) A VASP shall notify the Commission promptly of any matter that may affect the fitness and propriety of any controller, beneficial owner, director or senior officer.

Suspension, variation and revocation

24. (1) The Commission may suspend, vary, impose additional conditions on, or revoke a licence where it is satisfied that—

(a) the VASP or any other person on its behalf has contravened this Act or any other Act, regulations, rules, codes or licence conditions;

(b) the VASP has provided false or misleading information;

(c) a controller, beneficial owner, director or senior officer is not fit and proper;

(d) the VASP is insolvent, is likely to become insolvent, or cannot meet obligations to customers;

(e) continued operation poses a risk to consumers, market integrity or the reputation of the Islands;

(f) the VASP requests the Commission to alter or revoke their licence.

(g) 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 its business—

(i) has been convicted within the Islands of an offence;

(ii) has been convicted of an offence under this Act; or

(iii) has committed a breach of any rules made by the [Minister or Commission] under this Act for regulating the conduct of business by holders of licences; and

(h) it is otherwise in the public interest to do so.

(2) Before taking action under subsection (1), the Commission shall give the VASP notice of non-compliance and an opportunity to be heard, unless the Commission considers that urgent action is necessary to protect customers or the public.

(3) A notice of non-compliance shall specify—

(a) the provision of this Act or any AML/CFT/CPF legislation that was breached;

(b) the penalty payable under the licence;

(c) the period within which a penalty shall 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 Commission shall—

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

(b) suspend the licence; and

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

(5) Subject to Section 24(4)(a), all operations shall cease until the Commission advises the VASP that the suspension is lifted.

(6) If a VASP fails to comply with Section 24(4)(c), the Commission shall revoke the VASP licence, and the Commission shall serve a notice of the revocation to the VASP.

(7) A VASP whose licence is suspended or revoked shall comply with any directions issued by the Commission to ensure an orderly wind-up and protection of customer assets.

(8) Nothing in this Section limits the powers of the Commission under the FSCA to take enforcement action, including the imposition of administrative or supervisory penalties.

Surrender of Licence

25. (1) A VASP may apply to the Commission to surrender its licence in the prescribed form.

(2) The Commission may accept the surrender subject to such conditions as it considers necessary to protect customers, counterparties, or the public interest.

(3) The Commission may refuse to accept the surrender where—

(a) the VASP has outstanding obligations to customers or counterparties;

(b) the VASP is subject to ongoing investigations or enforcement proceedings; or

(c) acceptance would otherwise be contrary to the objects of this Act.

(4) A VASP whose licence is surrendered shall comply with any directions issued by the Commission to ensure an orderly wind-up and the safeguarding of customer assets.

Outsourcing and third-party arrangements

26. (1) A VASP shall not outsource a material function or activity, including custody, key management, technology operations, customer onboarding, compliance, or reserve custody (as applicable), unless it has—

(a) conducted due diligence on the VASP;

(b) ensured appropriate contractual protections, audit rights and access for the Commission;

(c) ensured that outsourcing does not materially impair the Commission's ability to supervise the VASP; and

(d) notified the Commission and obtained approval where required by rules or licence conditions.

(2) The VASP remains fully responsible for compliance with this Act in respect of any outsourced function.

(3) A person who fails to comply with subsection (1) commits an offence and is liable on conviction to the penalties prescribed in Section 99.

PART IV

ONGOING OBLIGATIONS OF LICENSED VASPS

General obligations

27. (1) A VASP shall at all times, in the manner prescribed by the Commission—

(a) conduct its business in a prudent manner, with integrity, due skill, care and diligence;

(b) deal with customers fairly and transparently;

(c) maintain adequate capital, human, technical and financial resources to discharge its services;

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

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

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

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

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

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

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

(k) maintain competence to provide the services of a VASPs;

(l) 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 43;

(m) take reasonable steps to ensure its beneficial owners are fit and proper;

(n) take reasonable steps to ensure its beneficial owners or any natural person employed by, or associated with, the VASP comply with this Act and all applicable laws in the Islands;

(o) take reasonable steps to ensure 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 Commission from time to time;

(p) take reasonable steps to ensure its beneficial owners or any natural person employed by, or associated with, the VASP comply with the conditions of the licence issued by the Commission;

(q) take reasonable steps to ensure its beneficial owners or any natural person employed by, or associated with, the VASP are competent to provide the services of a VASPs; and

(r) comply with all applicable sanctions laws and measures in force in the Islands, including those implementing international obligations.

(2) A VASP shall establish and maintain effective systems and controls appropriate to the nature, scale and complexity of its business.

Election of a director/authorised person

28. (1) A VASP shall elect a director, who will be responsible for the functioning of the VASP business in or from within the Islands.

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

(3) A VASP who intends to appoint a director shall apply to the Commission for its approval.

(4) The Commission may from time to time prescribe the functions of the appointed director.

(5) The Commission may from time to time prescribe the eligibility criteria for natural persons applying to become a director of a VASP.

Governance, risk management and internal controls

29. (1) A VASP shall establish governance arrangements that clearly allocate responsibilities for—

(a) oversight and management of risk;

(b) compliance and internal audit;

(c) custody and safeguarding arrangements;

(d) technology and cybersecurity; and

(e) outsourcing and third-party risk.

(2) The Commission may prescribe requirements for board composition, independent oversight, committees, and key function holders.

(3) A VASP shall maintain policies and procedures, reviewed at least annually, covering risk management, conflict management, customer disclosures, incident response and business continuity.

Capital, liquidity and financial resources

30. (1) A VASP shall maintain at all times capital and financial resources that are adequate for—

(a) the nature and scale of its activities;

(b) the risks to customers and to market integrity; and

(c) operational resilience and orderly wind-up.

(2) The Commission may prescribe minimum capital, liquidity buffers, insurance requirements, and stress testing requirements by licence class.

(3) The Commission may, in addition to any minimum capital prescribed under subsection (2), require a VASP to hold such additional capital as the Commission considers necessary having regard to the risk profile of the VASP.

(4) The Commission may require a VASP to maintain professional indemnity insurance, fidelity insurance, or other financial assurance (including bonding) in such amount and form as the Commission may prescribe.

Safeguarding of customer assets; segregation

31. (1) A VASP that holds or controls customer virtual assets or customer money shall segregate such assets and money from its own assets and money, in accordance with the requirements of Part XI of the Companies Act, or as otherwise prescribed.

(2) Customer assets shall be held—

(a) in a manner that clearly identifies them as customer assets; and

(b) in accounts or wallets that are protected against claims of the creditors of the VASP, to the extent permitted by law.

(3) A VASP shall maintain daily or such other periodic reconciliations as prescribed, and shall promptly investigate and rectify discrepancies.

(4) The Commission may require customer asset safeguarding arrangements to be subject to independent audit or assurance.

(5) A VASP, shall provide the Commission with online or automated real time read-only access to both its client and its own virtual asset transaction records.

(6) A VASP shall maintain a record of its clients and its own transactions at its head office for a period of not less than seven (7) years beginning from the date the transaction occurred.

Custody standards; private key management

32. (1) A VASP providing custody shall implement robust custody arrangements, including—

(a) secure private key generation, storage, access control and rotation;

(b) segregation of duties and multi-factor authentication;

(c) controls for transfers, including approvals and limits;

(d) resilience against loss, theft, compromise or unauthorised access; and

(e) arrangements for recovery and contingency, including key sharing or equivalent mechanisms.

(2) The Commission may issue detailed custody and key management standards, including requirements for cold storage, multi-signature, and third-party key management.

(3) A VASP shall disclose to customers, in a clear and prominent manner, the material features and risks of its custody arrangements.

Books, records, audit and reporting

33. (1) A VASP shall maintain accurate and complete books and records sufficient to enable the Commission to monitor compliance, including records of—

(a) transactions and transfers;

(b) customer onboarding and due diligence;

(c) custody arrangements and reconciliations;

(d) complaints and dispute resolution;

(e) incidents, breaches and outages;

(f) governance decisions and risk assessments; and

(g) its corporate records as prescribed by the Companies Act

(2) Records shall be kept for at least the period required under AML/CFT/CPF requirements and, in any event, not less than seven years.

(3) A VASP shall prepare annual financial statements and have them audited by an auditor approved by the Commission, unless otherwise exempted by the Commission. Financial statements shall be prepared in accordance with the requirements under the Companies Act.

(4) A VASP shall submit periodic regulatory returns and other reports as prescribed by the Commission.

(5) This Section when read together with Section 10 (Co-operation and Information Sharing), ensures that all VASPs remain subject to FATF-aligned AML/CFT and reporting obligations.

Market conduct, disclosures and advertising

34. (1) A VASP shall ensure that communications and advertising are fair, clear and not misleading.

(2) Prior to onboarding a customer, a VASP shall provide clear disclosures on—

(a) the nature of the service and the virtual assets involved;

(b) fees, spreads, charges and the basis of price formation;

(c) material risks, including volatility, liquidity, technology and custody risks;

(d) complaints and redress mechanisms; and

(e) whether the VASP acts as principal, agent or in another capacity.

(3) The Commission may prescribe standard risk warnings and disclosure formats.

Conflicts of interest

35. (1) A VASP shall identify, prevent, manage and, where relevant, disclose conflicts of interest, including conflicts arising from—

(a) proprietary trading or principal dealing;

(b) listing or virtual asset admission decisions;

(c) related-party arrangements and outsourcing; and

(d) incentives, remuneration and referral arrangements.

(2) The Commission may require structural separation, information barriers or other measures to manage conflicts.

Complaints handling and redress

36. (1) A VASP shall establish and maintain effective procedures for handling customer complaints and disputes, including timelines for acknowledgment and resolution.

(2) A VASP shall keep records of complaints and outcomes and shall report complaints data to the Commission as prescribed.

(3) The Commission may require participation in an ombudsman or alternative dispute resolution scheme where such a scheme is established.

Business continuity and orderly wind-up

37. (1) A VASP shall maintain business continuity and disaster recovery plans appropriate to its business, including arrangements for—

(a) system outages and cyber incidents;

(b) loss of critical staff of the VASPs; and

(c) rapid scaling during market stress.

(2) A VASP shall maintain an orderly wind-up plan that describes how it will cease operations while protecting customers and

returning customer assets. Such plan shall be aligned with the requirements of the Companies Act.

(3) The Commission may require periodic testing of business continuity plans and wind-up arrangements, which shall align with the requirements of the Companies Act.

PART V

COMPLIANCE

AML/CFT/CPF OBLIGATIONS AND THE FATF TRAVEL RULE

Compliance framework

38. (1) A VASP is a "financial business" under Schedule 2, Regulation 2 of POCA for AML/CFT/CPF purposes;

(2) AML/CFT/CPF requirements shall be consistent with the Financial Action Task Force Recommendations (FATF) relating to virtual assets and VASPs, and virtual assets transfers by VASPs, and applicable domestic requirements (the "travel rule").

(3) Where there is inconsistency between this Part and AML/CFT/CPF requirements, the stricter requirement applies.

(4) A VASP shall comply with the Proceeds of Crime Act and any regulations, codes or guidance issued thereunder, as applicable to financial business.

Transfers of virtual assets; travel rule

39. (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 business immediately and securely;

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

(2) A VASP shall implement measures to comply with the requirement to obtain, hold and transmit required originator and beneficiary information for transfers of virtual assets, consistent with the "travel rule".

(3) The travel rule requirements in subsection (1), apply to transfers of virtual assets at or above the de minimis threshold prescribed by the Commission; and the Commission must not prescribe a threshold higher than the equivalent of USD 1,000 in any currency.

(4) The Commission may prescribe—

(a) thresholds, data elements and formats;

(b) technical standards and secure messaging solutions; and

(c) requirements for unhosted wallet transfers and risk mitigation.

(5) A VASP shall establish policies for identifying and mitigating risks associated with transfers involving unhosted wallets or non-compliant counterparties.

(6) The information shall be made available upon the request of the Commission or any other competent authority.

(7) For the purposes of this Section, originator information includes:

(a) the name of the originator;

(b) the originator's virtual asset account number used to process the transaction or, in the absence of an account number, a unique transaction reference number that 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.

(8) 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 that permits traceability of the transaction.

(9) 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 is required to include the originator's account number or unique transaction reference number.

(10) Virtual asset transfers below [insert *de minimis* threshold] shall always be accompanied by the required originator information in subsection (7) and required beneficiary information in subsection (8).

(11) The information mentioned in subsection (8) does not need to be verified unless there are suspicious circumstances related to AML/CFT/CPF, in which case information pertaining to the customer should be verified.

(12) The originating VASP shall maintain all originator and beneficiary information collected in accordance with the recordkeeping requirements in Section 41.

(13) The originating VASP shall not execute the virtual asset transfer if it does not comply with the above requirements.

(14) The Commission may issue policies for identifying and managing transactions lacking required information.

Intermediary VASPs

40. (1) An intermediary VASP shall ensure all originator and beneficiary information that accompanies a virtual asset transfer is securely retained.

(2) Where technical limitations prevent the required originator or beneficiary information accompanying a virtual asset transfer from being retained, the intermediary VASP shall keep a record, for at least seven (7) years, of all the information received from the originating VASP or another intermediary VASP.

(3) 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.

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

(5) 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 jurisdictions in which they operate, directly or through their agents.

(6) 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 the beneficiary sides in order to determine whether a suspicious transaction report (STR) has to be filed; and

(b) file an STR in any country affected by the suspicious virtual asset transfer and make relevant transaction information available to the Financial Intelligence Unit.

(7) A VASP shall, in processing virtual asset transfers—

(a) take appropriate measures to identify and comply with sanctions obligations applicable in the Turks and Caicos Islands;

(b) implement measures to freeze or restrict transactions involving designated persons or entities, where required by applicable law; and

(c) ensure that transactions involving designated persons or entities are reported in accordance with applicable legal requirements.

(8) For the purposes of this Act, the term “suspicious transaction report” or “STR” has the same meaning in this Act as given under the Proceeds of Crime Act, and no separate reporting regime is created under this Act,

PART VI

INITIAL VIRTUAL ASSET OFFERINGS ISSUANCE

Application of this Part

41. (1) This Part applies to an initial virtual asset offering conducted in or from within the Islands.

(2) This Part does not apply to an offering of securities or other regulated instruments that is subject to the Investment Dealers (Licensing) Act or the Mutual Funds Act (as applicable), except to the extent that the Commission otherwise authorises.

(3) The Commission may exempt an offering from specified requirements where appropriate.

Requirement for notice or approval

42. (1) A person shall not offer or issue a virtual asset to the public unless—

(a) the person has notified the Commission of the information prescribed by Schedules 4 to 5; and

(b) the Commission has issued an approval or non-objection, where required by regulations or Commission rules.

(2) The Commission may prescribe any other categories of virtual asset offerings requiring approval and categories requiring notification only.

(3) A person who contravenes subsection (1) commits an offence and is liable on conviction to penalties prescribed in Section 99.

White Paper and disclosure obligations

43. (1) Where the Commission issues an approval or non-objection under Section 42(1)(b), a VASP shall prepare and publish a White Paper that is fair, clear and not misleading and contains prescribed information in Schedule 5, including—

(a) the identity, governance and financial information of a VASP;

(b) the project description, virtual asset characteristics, rights and obligations;

(c) use of proceeds and allocation of virtual assets;

(d) material risks, including technology, cybersecurity and market risks;

(e) arrangements for custody of proceeds and any reserve assets; and

(f) AML/CFT/CPF requirements and any restrictions on participation.

(2) The White Paper disclosure structure is illustrated in Schedule 6.

(3) The Commission may require independent review of a White Paper or supporting technical or legal opinions.

(4) The VASP shall update the White Paper where there is a material change and shall notify the Commission.

(5) The Commission may prescribe requirements in relation to the form and timing of such information as it considers appropriate.

Ongoing obligations of VASPs

44. (1) In addition to Section 24, a VASP shall comply with ongoing obligations prescribed by the Commission, including—

(a) reporting on use of proceeds;

(b) updates on project milestones and governance;

(c) incident reporting where relevant; and

(d) maintaining appropriate records and audit trails.

(2) The Commission may impose conditions or directions to protect participants.

Marketing and distribution restrictions

45. (1) Marketing communications relating to an initial virtual asset offering shall be fair, clear and not misleading.

(2) The Commission may impose restrictions on marketing to retail persons, including cooling-off periods, suitability assessments, investment limits or other measures.

(3) A VASP shall not engage in misleading, deceptive or manipulative conduct in relation to an offering.

Civil liability for misstatements

46. (1) Where a person suffers loss as a result of a material misstatement or omission in a White Paper, the VASP and any person responsible for the White Paper may be liable to compensate that person, subject to defenses prescribed under this Act and by law.

(2) This Section is without prejudice to any criminal liability for fraud or other offences.

(3) The Commission may issue guidance or codes of practice in relation to marketing and distribution of virtual assets, including guidance having regard to relevant international standards and best practices.

PART VII

TECHNOLOGY, CYBERSECURITY AND OPERATIONAL RESILIENCE

ICT and cyber risk management

47. (1) A VASP shall establish and maintain an ICT and cyber risk management framework that is proportionate to the nature, scale and complexity of its activities.

(2) The framework shall include—

(a) governance and accountability for ICT risk;

(b) asset inventory and configuration management;

(c) access control, authentication and privilege management;

(d) secure software development and change management;

(e) monitoring, logging and threat detection;

(f) vulnerability management and patching; and

(g) third-party and supply-chain risk management.

(3) The Commission may prescribe minimum ICT and cybersecurity standards.

(4) The Commission may make guidelines, codes or standards in relation to this Section.

(5) In this Section, "information and communication technology" or "ICT" means systems, networks, hardware, software, and data infrastructure used to support the operation of virtual asset activities.

Incident and breach reporting

48. (1) A VASP shall notify the Commission as soon as practicable, and in any event within the prescribed time, of any material incident, including—

(a) cybersecurity breach or attempted breach;

(b) loss, theft or compromise of private keys or customer assets;

(c) significant service outage or disruption;

(d) data breach involving personal or confidential information; and

(e) any other incident prescribed by the Commission.

(2) A notification shall include information on impact, root cause, remedial actions and customer communications.

(3) The Commission may require an independent post-incident review.

Systems assurance and independent testing

49. (1) A VASP shall arrange for periodic independent testing of its systems and controls, including penetration testing and security assessments, in accordance with Commission standards.

(2) Where a VASP operates smart contracts or critical on-chain components, the Commission may require independent smart contract audits, formal verification, and ongoing monitoring.

(3) A VASP shall provide the results of testing to the Commission upon request.

(4) The Commission may require a licensee to undertake independent systems assurance, including a cybersecurity assessment, in accordance with the standards set out in Schedule 12.

(5) The Commission shall prescribe fees under this Section, as applicable.

Outsourced technology and cloud services

50. (1) A VASP shall ensure that any outsourced technology provider or cloud VASP complies with security and resilience requirements and provides appropriate audit rights and access for the Commission.

(2) The Commission may require that certain data be stored or accessible in the Islands or in approved jurisdictions.

Data governance and privacy

51. (1) A VASP shall implement data governance policies, including classification, retention, access control and secure disposal.

(2) A VASP shall protect personal and confidential information and shall comply with applicable domestic and international data protection and privacy laws.

Financial system integration and cross-border compatibility

52. (1) A VASP shall ensure that its systems, processes, and governance arrangements are designed to support interoperability with—

(a) domestic payment systems, financial businesses, and regulatory frameworks; and

(b) foreign payment networks, virtual asset regimes, and supervisory authorities, where applicable.

(2) Virtual assets shall be designed for seamless integration with financial businesses, central banks, and VASPs requirements.

(3) VASPs shall ensure compliance with international financial messaging standards, including ISO 20022, to enable cross-border compatibility.

(4) virtual assets shall support cross-chain interoperability mechanisms such as atomic swaps, bridge protocols, and inter-block communication standards.

(5) On-chain identity verification shall be integrated to meet regulatory requirements without compromising decentralization.

(6) The Commission may issue guidance relating to—

(a) compliance with ISO 20022 including messaging standards and operational integration for stablecoin systems; and

(b) the application of conflict of law principles clarifying that where multiple legal frameworks apply, the stricter rule will prevail.

(7) In this Section "ISO 20022" means the international standard for financial messaging developed by the International Organization for Standardization, providing a common data model and message format for financial transactions.

PART VIII

REGULATORY SANDBOX

Establishment of regulatory sandbox

53. (1) The Commission may establish a regulatory sandbox to facilitate the testing of any innovative virtual asset products, services or business models under controlled conditions.

(2) The Commission may publish a sandbox framework setting out eligibility, application procedures, testing parameters, safeguards and reporting requirements.

(3) The sandbox framework published under subsection (2) shall be read together with, and may be supplemented by the requirements in Schedule 15 and other prescribed requirements according to, among other consideration, the type of business model and intended virtual activities to be conducted.

(4) Without limiting subsection (2), the sandbox framework and Schedule 15, the Commission may make provisions for—

(a) eligibility criteria and application requirements;

(b) testing plan requirements;

(c) customer protection measures;

(d) safeguarding and custody of client assets;

(e) ICT, cybersecurity and operational resilience;

(f) reporting obligations and notifiable events;

(g) limits and conditions applicable to sandbox testing; and

(h) exit, wind-up and transition to full licensing.

(5) Compliance with the sandbox framework and Schedule 17 (including Annexes A and B) and any other prescribed requirements, is a condition of sandbox authorisation, and failure to comply constitutes grounds for action under Section 94 and any other applicable enforcement powers.

Sandbox authorisation and conditions

54. (1) The Commission may grant a sandbox authorisation to an applicant for a specified period and subject to conditions, including

limits on customers, transaction volumes, jurisdictions, and risk mitigation measures.

(2) The Commission may, for the purposes of sandbox testing, modify or waive specified requirements of this Act or regulations, but must not waive—

(a) core AML/CFT/CPF requirements; or

(b) requirements necessary to prevent fraud, protect customer assets, or manage systemic risk.

(3) A sandbox participant shall provide periodic reports to the Commission and shall notify the Commission of material incidents, as prescribed.

(4) The fees payable in respect of an application for, the grant of, renewal of, or any variation to a sandbox authorisation shall be as prescribed by the Commission.

Exit and transition

55. (1) A sandbox authorisation may be terminated by the Commission, or surrendered by the participant, in accordance with sandbox conditions.

(2) On termination, the participant shall cease the sandbox activity and comply with any directions for customer protection and orderly wind-up.

(3)Where a sandbox participant intends to transition to full licensing, the Commission may set expedited procedures, without prejudice to full assessment requirements.

PART IX

STABLECOINS

Scope of, and interpretation for, this Part

56. (1) This Part applies specifically to any person who carries on stablecoin activities as a business in or from within the Islands, as prescribed by Sections 63 and 64.

(2) For the avoidance of doubt under the VASP regime in the Islands, an issuer of stablecoins under this Part is subject to the provisions as prescribed in Parts 1 to 8, of this Act.

Interpretation of Part 9

57. In this Part of the Act, unless the context otherwise requires—

"algorithmic stablecoin" means a type of stablecoin that seeks to maintain a stable value through the use of algorithms, smart contracts, or protocol-defined rules that automatically adjust the supply or demand of the stablecoin—without direct backing by fiat currency, commodity reserves, or other tangible assets and which may rely on mechanisms such as rebasing, seigniorage

models, or the use of volatile crypto-assets as collateral to stabilise prices;

"decentralised protocol" has the meaning assigned in section 62(11);

"de-pegging" means the loss or breakdown of the price stability mechanism of a stablecoin, resulting in the coin trading at a material variance from its intended peg;

"DAO" refers to Decentralised Autonomous Organization(s) and has the meaning assigned in section 62(10) ;

"Oracle" means a blockchain-based system or service that connects the stablecoin ecosystem to external data sources, enabling it to access and utilise information from the real world. An Oracle sources, verifies and communicates data originating outside the stablecoin ecosystem to be used by and for the stablecoin processes;

"permitted reserve assets" has the meaning assigned in Section 73;

"reserve" means the pool of assets that an issuer holds to back the value of the issued stablecoin to ensure its stability relative to the referenced currency or asset;

"secure coding" means techniques used to prevent vulnerabilities in software design and implementation;

"stablecoin" refers to a class of virtual asset designed to maintain a stable value by referencing the value of one or more assets, including official currencies, commodities, or other financial instruments, which is transferable electronically using distributed ledger technology and functions as a store of value, unit of account, or medium of exchange;

"stablecoin activities" has the same meaning as assigned in Section 63;

"stablecoin arrangement" means a set of functions, rules, roles and governance relating to the issuance, redemption, transfer, stabilisation mechanism, reserve management, and operation of a stablecoin;

"stablecoin ecosystem" means the interconnected components, participants, and applications that are involved in the creation, management and use of stablecoins;

"stablecoin issuance" means the making of a stablecoin publicly available for purchase or acquisition by an issuer;

"tier 0 – tier 3" inclusively, has the same meaning as assigned in Section 68;

"tiered licensing framework" means a risk-based approach where licensing requirements differ based on the scale of issuance, type of stablecoin issued, risk exposure (AML/CFT/CPF, market stability, and technological resilience) and the nature of the issuing entity;

"issuer" in this Part means a VASP that issues, offers, redeems or otherwise creates a stablecoin as part of a stablecoin arrangement;

Scope and application of this Part

58. (1) This Part applies to licensed VASPs listed under subsection (3).

(2) This Act governs both retail and wholesale stablecoins, including those used for—

(a) domestic and cross-border transactions;

(b) clearing and settlements;

(c) programmability; and

(d) embedded or automated financial functions (e.g. lending, staking, and insurance features).

(3) Stablecoins may only be issued, governed, or managed by—

(a) legal persons that meet the licensing requirements and obligations set out in Part 3 of this Act; and

(b) any other authorised entities, including—

(i) financial institutions, as defined in the FSCA;

(ii) DAOs;

(iii) legal persons issuing algorithmic, rebase, or protocol-native stablecoin; or

(iv) legal persons that manage stablecoins designed to maintain value stability through decentralised or non-traditional mechanisms, including price oracles, algorithmic market operations, or autonomous smart contracts or hybrid arrangements are within scope to the extent that they conduct any activity described in (a) or (b).

(4) The Commission may supervise and oversee algorithmic stablecoins, in a similar manner as prescribed for tiered classification, prudential standards, and regulations under Section 101.

(5) Licensing criteria for stablecoin issuers, including algorithmic variants, shall meet fit and proper standards under Section 70, with enhanced scrutiny for algorithmic mechanisms to ensure stability and reserve adequacy.

(6) For the purpose of this Part: legal persons identified in subsections 3(a) and (b) are VASPs or "issuers" and both terms are used interchangeably; and

(7) For the purposes of this Section, "intermediary" means any natural or legal person that facilitates the issuance, distribution, exchange, custody or redemption of stablecoins on behalf of an issuer or user, including digital asset exchanges, wallet providers, custodians, and payment processors.

Classification of stablecoins

59. (1) Subject to section 65(1), stablecoins may be classified into the following, with each class subject to distinct licensing and regulatory requirements—

(a) Payment stablecoins that aim to maintain a stable value by referencing a single official currency and redeemable at par value;

(b) Reserve-backed stablecoins that reference a combination of virtual assets, including fiat currencies, commodities, or other financial instruments; and

(c) Yield-bearing stablecoins that reference any mechanism embedded in the stablecoin or offered by the issuer enabling the holder to receive income, interest, or rewards in return for holding, staking, or locking the stablecoin, whether such returns are fixed, variable, or algorithmically determined.

(2) The Commission may do either or both of the following pertaining to stablecoins—

(a) specify a unit of account or store of economic value; and

(b) specify a digital representation of value, or class of digital representations of value.

Regulating stablecoin issuance

60. (1) A stablecoin may be issued by—

(a) minting a digital token on a distributed ledger network and assigning it to a user account; or

(b) any other approved issuance mechanism authorised by the Commission.

(2) The issuer shall maintain accurate, real-time records of all issuance, distribution, and redemption transactions of stablecoins, and provide such records to the Commission upon request.

(3) The issuance of stablecoins with yield-bearing features shall be subject to additional or enhanced disclosure, transparency, and risk management obligations as prescribed by the Commission, including the clear identification of—

(a) the source of yield generation;

(b) the issuers responsible for yield distribution;

(c) any contractual or algorithmic mechanisms governing the yield; and

(d) and associated risks of loss, volatility, or de-pegging.

Prohibition on stablecoins issuers

61. (1) In line with Sections 4 and 12, a natural person—

(a) shall not offer or issue stablecoins as a business in the Islands; and

(b) shall issue stablecoins in the Islands only in the manner set out under this Act.

Stablecoin activities

62. (1) For the purposes of this Part, a person shall not carry on or purport to carry on any stablecoin activities as a business in the Islands unless that person is in compliance with the requirements of Part 1 to Part 8 of this Act and any conditions imposed by the Commission.

(2) For the purposes of this Part, a person carries on a stablecoin activity if it—

(a) issues a stablecoin in the course of business;

(b) issues a stablecoin in any location in the course of business, and the stablecoin purports to maintain a stable value with reference to a specific currency or basket of assets; or

(c) offers or facilitates yield-bearing features on stablecoins, including through protocols, platforms, or if such activity constitutes a virtual activities under Section 13; and

(3) A reference to a stablecoin activity is to be construed accordingly and as prescribed by the Commission.

(4) This Section also applies to DAO-Issued and niche stablecoin—

(a) issued, governed, or managed by a DAO;

(b) structured as an algorithmic, rebase, or protocol-native stablecoin; or

(c) designed to maintain value stability through decentralised or non-traditional mechanisms, including price oracles, algorithmic market operations, or autonomous smart contracts.

(5) DAO-issued or niche stablecoins shall be subject to the applicable Tier classification and supervision under this Act, unless explicitly exempted by the Commission.

(6) Subject to subsection (7), a DAO or decentralised protocol shall not be exempt from regulatory obligations on the basis of its structure alone.

(7) Where there is no identifiable Legal Person, the DAO shall appoint an authorised person, compliance agent, or legal representative with authority to interface with the Commission.

(8) The Commission may prescribe classes of stablecoins or arrangements that are prohibited or restricted, including algorithmic stablecoins or yield-bearing stablecoins, where the Commission considers that the risks cannot be adequately mitigated.

(9) A person who contravenes subsection (1) commits an offence and is liable on conviction to the penalties prescribed in Section 99.

(10) For the purposes of this section, a DAO refers to a blockchain-based governance or operational arrangement that uses smart contracts or distributed decision-making mechanisms rather than traditional centralised management structures.

(11) In this section, a decentralised protocol refers to a blockchain-based system that operates through distributed infrastructure, automated processes or community-based participation without reliance on a single central controlling entity.

Carrying on stablecoin business

63. (1) For the purposes of this Section, a person, authorised person or agent on behalf of a legal entity shall not carry on or purport to issue stablecoins in or from within the Islands unless that person holds a valid licence granted under one of the license classes specified as prescribed.

(2) For the purposes of this Part, stablecoin activities includes where—

(a) an issuer actively markets, whether domestically or internationally, to the public that such issuer carries on, or purports to carry on, such activity; and

(b) the activity, if carried on within a regulated financial framework, would constitute a stablecoin activity.

(3) Subsection (1) applies in relation to an issuer regardless of—

(a) whether the carrying on, or purported carrying on, of an activity mentioned in subsection (2)(a) is actively marketed by the issuer or another person on behalf of the issuer; and

(b) whether the activity mentioned in Section 9(2)(a) is carried on or not.

(4) The Commission may, after consulting relevant financial authorities, include an activity for the purposes of this Section.

(5) In exercising a power to specify an activity under subsection (4), the Commission must, in addition to any other matters that the Commission considers relevant, have regard to—

(a) whether the activity is, or is likely to become, material to the monetary or financial stability of the Islands;

(b) whether the activity is, or is likely to become, material to the functioning of the Islands as a financial services jurisdiction; and

(c) the matters of significant public interest, including—

(i) the protection of customers, investors, or end-users of stablecoin systems;

(ii) the prevention of financial crime, including money laundering, terrorist financing, and proliferation financing;

(iii) systemic risks arising from market concentration, technological failure, or governance weaknesses;

(iv) the promotion of competition, innovation, and financial inclusion; and

(v) the upholding of public trust and confidence in the digital financial system.

(6) For the purposes of subsection (5)(a), an activity is or is likely to become material to monetary or financial stability, if the occurrence of any significant disruption to the carrying on of the activity is likely to adversely affect financial system stability.

(7) For the purposes of subsection (5)(b), an activity is or is likely to become material to the functioning of a financial service jurisdiction, if the occurrence of any significant disruption to the carrying on of the activity is likely to—

(a) adversely affect the role of the Islands as a financial services jurisdiction; or

(b) cause systemic disruption to the financial system.

(8) For the purposes of subsection (5)(c), the following matters are to be regarded as matters of significant public interest—

(a) whether the occurrence of any significant disruption to the carrying on of the activity is likely to adversely affect the public's confidence in the financial system; and

(b) whether the occurrence of any significant disruption to the carrying on of the activity is likely to adversely affect day-to-day commercial activities.

Licensing required for stablecoin activities

64. (1) A legal person shall not issue, or hold themselves out as issuing, stablecoins unless that Person—

(a) is duly licensed as an issuer of stablecoins under this Part; and

(b) complies with all requirements imposed on a VASP under Parts 1 to 8 of this Act and any conditions imposed on a VASP by the Commission.

(2) To apply for an issuer licence, the applicant shall be a legal person registered or licensed in the Islands or incorporated outside the Islands, as prescribed in this Act.

(3) An application for a licence to carry on business as an issuer shall be in the form and manner prescribed in Schedules 2 and 16 or as determined by the Commission.

(4) The Commission may grant a licence to an applicant if it is satisfied that—

(a) the applicant is fit and proper to carry on stablecoin activities;

(b) appropriate arrangements are in place for reserve management, governance, risk control, and customer protection; and

(c) the applicant meets any financial, technological, and operational criteria prescribed by rules or directives.

(5) The Commission may prescribe rules—

(a) classes or tiers of stablecoin licences;

(b) exemptions or modifications for experimental, limited-scale, or sandbox activities; and

(c) procedures for application, renewal, suspension, or revocation of licences.

(6) Any issuer that is licensed in the Islands or a country that is deemed by the Commission to be equivalent in substance and effect to the requirements of this Act may apply for a registration in the Islands in order to offer its services or stablecoins to residents or nationals of the Islands.

Application for a VASP stablecoin licence

65.(1) An application shall be made in the prescribed form and be accompanied by such information and such fee as may be as prescribed by Regulations.

(2) An application shall include, at a minimum—

(a) information specified in Schedules 1 and 2; and

(b) any other information prescribed by the Commission.

(3) The Commission may require the applicant to provide additional information, clarifications or documents within a specified period.

Obligations for licensed stablecoin issuers

66. (1) A person licensed under this Part shall conduct its stablecoin activities in a manner that promotes financial integrity, customer protection, and systemic stability.

(2) Issuers shall comply with all obligations imposed under Parts 1 to 8 of this Act.

(3) An issuer must, in addition to subsection (2)—

(a) comply with the obligations imposed on VASPs generally of initial virtual asset offerings under Part 6;

(b) operate as fiduciaries with respect to customer holdings and shall act in the best interest of stablecoin holders,

prioritising the protection, safekeeping, and liquidity of reserve assets;

(c) treat customers equally;

(d) include in its White Paper key information including the information prescribed in Schedules 4 and 5;

(e) publicly disclose guidelines on implementation timelines imposed on issuers by the Commission; and

(f) meet the reserve management and transparency obligations prescribed in Sections 71 to 83.

Tiered licensing framework for stablecoin issuers

67. (1) The Commission may implement a tiered licensing framework for licensed stablecoin issuers, based on risk exposure and systemic importance.

(2) A person authorised under a VASP licence to carry on stablecoin activities shall be classified by the Commission into one of the following tiers—

(a) Tier 0;

(b) Tier 1;

(c) Tier 2; or

(d) Tier 3.

(3) Classifications under subsection (2) shall be determined having regard to—

(a) the scale of stablecoin issuance;

(b) the aggregate value of stablecoins in circulation;

(c) the nature and composition of reserve assets;

(d) the number and geographic distribution of users;

(e) interconnectedness with financial institutions or payment systems;

(f) systemic, prudential and operational risk exposure; and

(g) such other criteria as may be prescribed in Schedule 5 or by regulations.

(4) Tier 1 issuers may be identified by the following characteristics—

(a) significant market reach and financial system implications;

(b) minimum quantitative thresholds as prescribed in Schedule 7; and

(c) significant cross-border operations.

(5) Tier 1 issuers may be subject to a full range of prudential, governance, disclosure, and cross-border supervisory standards.

(6) Tier 2 issuers may be identified by the following characteristics—

(a) issuers of moderate-scale stablecoins; and

(b) minimum quantitative thresholds as set out in Schedule 7.

(7) Tier 2 issuers may be required to meet baseline capital, reserve, AML/CFT, and governance standards.

(8) Tier 3 issuers may be identified by the following characteristics—

(a) issuers for closed-loop stablecoin ecosystems;

(b) limited use cases; and

(c) minimum quantitative thresholds as set out in Schedule 7.

(9) Tier 3 issuers may be subject to simplified licensing with AML/CFT, customer protection, and IT security obligations.

(10) The duration of a licence issued to a Tier 1, 2 or 3 issuer shall be subject to the discretion of the Commission.

(11) Tier 0 issuers may be identified by the following characteristics—

(a) issuers operating under a regulatory sandbox or a DAO with capped issuance; and

(b) minimum quantitative thresholds as set out in Schedule 7.

(12) The duration of a licence issued to a Tier 0 issuer is twelve (12) months and may only be renewed once.

(13) The Commission may prescribe thresholds and criteria for tiers, including outstanding liabilities, transaction volume, number of users, interconnectedness, and cross-border reach.

(14) Tiering shall be used to calibrate prudential requirements, reporting, disclosure, and supervisory intensity.

(15) The Commission shall publish guidance setting out the quantitative and qualitative thresholds applicable to each tier.

(16) A stablecoin issuer shall comply with the requirements applicable to the tier into which it is classified.

Tiered governance and risk regulatory requirements

68. (1) For the purposes of licensing and regulatory supervision of issuers under this Act, such issuers may be classified into the following tiers based on their size, systemic importance, risk exposure, and issuance model, as appropriate, and as prescribed by Schedule 5.

(2) Tier 1 Classification includes financial businesses or entities whose stablecoin activities are systemically important, including those—

(a) with high transaction volume or customer base;

(b) with wholesale, cross-border, or interbank use cases; or

(c) whose failure would pose a material threat to financial stability.

(3) Where the financial businesses or entities fall within the Tier 1 classification, the Commission may be the Prudential Regulator.

(4) Tier 2 Classification includes VASPs and financial businesses offering stablecoin services to retail or institutional customers at scale, but without systemic impact, and includes—

(a) non-bank financial businesses;

(b) VASPs, or e-money institutions; and

(c) custodial VASPs.

(5) Where the issuer falls within the Tier 2 classification, the competent authority may be either the Prudential Regulator.

(6) Tier 3 Classification includes limited or niche issuers or entities issuing stablecoins with limited scope or experimental use, including—

(a) pilot or sandbox programmes;

(b) Algorithmic issuers or DAOs with capped issuance or user thresholds; or

(c) community or niche use cases.

(7) for the purposes of subsection (6)(b) algorithmic stablecoins—

(a) shall be assessed by the Commission and, unless otherwise demonstrated to have equivalent reserve and stabilisation mechanisms, may default to Tier 3 classification to operate under a conditional licence; or

(b) relying solely on endogenous assets may be disallowed by default unless expressly permitted, and explicitly require enhanced obligations.

(8) Issuers of algorithmic stablecoins shall meet enhanced obligations under this Act, including—

(a) disclosure of algorithmic mechanisms and failure scenarios;

(b) independent code audit and stress testing;

(c) contingency plans for market volatility and de-pegging events;

(d) reserve buffers, if hybrid collateral models are used;

(e) enhanced investor risk disclosures; and

(f) any other obligations that the Commission may deem fit.

(9) DAO-issued stablecoins shall be classified as Tier 3 stablecoins unless the issuer can demonstrate to the satisfaction of the Commission—

(a) the existence of verifiable, transparent governance structures;

(b) the appointment of one or more identifiable responsible persons for compliance;

(c) implementation of multi-signature or over treasury and protocol changes;

(d) periodic independent audits of reserve assets and Smart Contracts; and

(e) the ability to meet reserve, redemption, and disclosure requirements under this Act.

(10) Where a DAO-issued stablecoin is unable to meet the requirements of this Act, the Commission may prohibit its issuance, promotion, or access through VASPs in the Islands.

(11) The Commission may, by public notice—

(a) permit DAO-issued or algorithmic stablecoins to operate under a conditional licence or within a regulatory sandbox;

(b) impose enhanced disclosure, AML/CFT screening, and customer protection requirements; and

(c) require real-time monitoring and reporting and restrict retail access where appropriate.

(12) Where an entity falls within the Tier 3 classification, the Commission may determine the appropriate supervisory authority including—

(a) the Commission as VASP supervisor;

(b) the regulatory sandbox or innovation unit; or

(c) such other authority or framework as prescribed by Regulations, having regard to the nature and risk of the arrangement.

(13) The Commission may establish protocols for joint supervision and information sharing, particularly where an issuer meets multiple tier criteria or evolves across tiers.

(14) Issuers may be subject to reclassification by the Commission based on periodic risk assessments, market activity, or breaches of systemic thresholds, subject to appeal and transition rules under Sections 102 and 105.

(15) The Commission may amend the tiered licensing framework from time to time by adding new tiers or amending the description of tiers as it considers necessary.

(16) In subsection (9) M-of-N refers to a cryptographic or operational control mechanism whereby a minimum number (M) of authorised parties or credentials, out of a total number (N), are required

to approve, access, or execute a sensitive operation or function to ensure that fewer than M participants cannot successfully perform the operation.

Inter-Tier Transition and Reclassification

69. (1) Issuers shall monitor thresholds quarterly and notify regulators within thirty (30) days of nearing a higher tier.

(2) Issuers that temporarily exceed the transaction volume, reserve size or user base thresholds applicable to their current licensing tier must—

(a) notify the Commission upon identifying a breach or the risk of a breach;

(b) indicate to the Commission whether the breach was incidental and reversible and submit a remediation plan within five (5) business days of the breach; and

(c) cease any further expansion of operations beyond the licensed limits until the Commission approves either a return to compliance or a progression to a higher tier.

(3) Where a formal transition to a higher tier is intended, issuers shall indicate that intention to the Commission and submit a transition plan within five (5) business days of indicating such intention.

(4) Issuers shall incorporate in their business continuity plans reasonable forecasting and escalation procedures for potential tier breaches, including contingency for rapid compliance with higher-tier regulatory obligations.

(5) Issuers shall submit reclassification documentation if [80%] of a higher-tier threshold is reached.

(6) The Commission may reclassify issuers up or down and conduct reassessment within [sixty (60) days].

(7) The Commission may apply provisional tier status during reclassification with temporary compliance flexibility.

(8) The Commission may, on its own initiative or upon application by a licensed stablecoin issuer, reclassify the issuer into a different tier where—

(a) the issuer exceeds or falls below prescribed quantitative thresholds;

(b) there is a material change in business model, risk profile or scale of operations;

(c) systemic risk considerations so require; or

(d) it is otherwise in the public interest to do so.

(9) Before reclassifying an issuer under subsection (1), the Commission must—

(a) give written notice of its intention to reclassify;

(b) specify the reasons for the proposed reclassification; and

(c) afford the issuer a reasonable opportunity to make representations.

(10) A reclassification shall take effect on the date specified in the notice, and the issuer shall comply with the requirements applicable to the new tier within such transitional period as the Commission may specify.

(11) The Commission may prescribe transitional prudential or reporting measures to ensure orderly adjustment between tiers.

Fit and proper requirements and tiered approach to prudential standards

70. (1) The Commission shall assess the fitness and propriety of applicants and licensees in accordance with criteria set out in this Act and under AML/CTF/CPF requirements.

(2) The Commission may apply a tiered approach to prudential requirements, in accordance with the classification of issuers under Schedule 1, ensuring that—

(a) entities with systemic or large-scale operations are subject to enhanced prudential obligations; and

(b) smaller or niche issuers are not subject to disproportionate regulatory burdens, while maintaining minimum standards of competence, integrity, and compliance.

(3) Every licensed stablecoin issuer, and its controllers, beneficial owners, directors and senior officers, shall be and remain fit and proper persons in accordance with Section 20 and this Act.

(4) In determining fitness and propriety under this Part, the Commission shall have regard to—

(a) competence and experience relevant to reserve management, custody, technology and financial risk;

(b) integrity, reputation and financial soundness;

(c) governance capability proportionate to the issuer's tier classification; and

(d) capacity to comply with AML/CFT/CPF requirements.

(5) Higher-tier stablecoin issuers may be subject to enhanced governance and prudential standards, including—

(a) independent directors;

(b) specialised board committees;

(c) dedicated risk, compliance and audit functions; and

(d) enhanced reporting and disclosure requirements.

(6) Failure to maintain fitness and propriety constitutes grounds for administrative and supervisory actions under Section 94 or any other applicable power.

Obligation to maintain reserves

71. (1) A licensed issuer shall at all times maintain reserve assets sufficient to meet all outstanding redemption obligations in respect of issued stablecoins;

(2) Reserved assets shall comprise only high-quality liquid assets or cash equivalents prescribed or approved by the Commission;

(3) For the avoidance of doubt, any lending, staking, insurance or similar feature offered in connection with a stablecoin constitutes a separate activity requiring appropriate authorisation under this Act or any other applicable law.

Permitted reserve assets

72. (1) The Commission may prescribe permitted reserve assets, including limits and concentration requirements, taking into account liquidity, credit quality and market risk.

(2) Reserve assets shall include—

(a) fiat currency held in deposit accounts with regulated financial businesses;

(b) government securities rated AA or higher, with a remaining maturity not exceeding ninety (90) days;

(c) units or shares in public money-market funds investing in government debt securities and short-term cash deposits in commercial banks subject to Commission-agreed limits, credit ratings and legal arrangements; and

(d) other high-quality liquid assets as may be approved by the Commission, subject to liquidity and concentration requirements.

(3) Permitted reserve assets shall not include—

(a) corporate equities;

(b) virtual assets;

(c) any asset issued by a related party;

(d) illiquid or encumbered instruments;

(e) any other assets determined by the Commission.

(4) In this Section "high-quality liquid assets" means assets that can be easily and quickly converted into cash with little or no loss of value. The term is primarily used in the context of the liquidity coverage ratio under the Basel III banking regulations, which require banks to hold enough high-quality liquid assets to cover net cash outflows for thirty (30) days in a stress scenario.

Custody and segregation of reserves

73. (1) Reserve assets shall be held in segregated accounts for the benefit of stablecoin holders and shall not be used for the issuer's own account, pledged, encumbered, or rehypothecated, except as permitted by Commission rules or financial businesses that meet minimum capital adequacy and custody requirements set by the Commission.

(2) Issuers shall ensure that reserve assets are legally protected from claims by creditors of the issuer in the event of insolvency.

(3) The issuer shall maintain robust valuation, reconciliation and internal control processes for reserves and shall perform reconciliations at least daily, or as prescribed by the Commission.

(4) Reserve assets shall be held with custodians approved by the Commission and in accordance with custody standards prescribed by the Commission.

(5) Reserve assets held in segregated accounts are held on trust for the benefit of the holder of the stablecoins.

(6) The Commission may require diversification across custodians and may require that reserve assets be held in specified jurisdictions or with specified types of regulated institutions.

Redemption rights and operational requirements

74. (1) An issuer shall provide a clear and enforceable right of redemption at par value, subject to any permitted fees and timeframes prescribed by the Commission.

(2) The issuer shall maintain policies and systems to meet user redemption requests under stress, including liquidity management, stress testing and contingency funding arrangements.

(3) Each issuer shall honour user redemption requests in a timely, transparent, and reliable manner, subject to the terms and conditions approved by the Commission.

(4) Any restrictions on redemption, including gates, delays or suspension, shall be prohibited unless—

(a) permitted by Commission rules;

(b) clearly disclosed to users; and

(c) approved by the Commission for Tier 0 arrangements or where otherwise required.

(5) Issuers shall ensure that redemption of stablecoins into fiat currency is available within one business day (T+1), without undue delay or material discount.

(6) The Commission may issue a Guidance Note on redemption and convertibility in Schedule 8.

(7) For the purposes of this Part "gates" or "gating" means any measure, whether automated or discretionary, implemented by an issuer or any person acting on its behalf, or by any intermediary, that

temporarily restricts, suspends, delays, or imposes quantitative limits on—

(a) the redemption of a stablecoin for fiat currency or other reserve assets at par; or

(b) the withdrawal, transfer, or settlement of stablecoins or related customer funds, including by way of redemption windows, daily or periodic caps, queues, extended settlement times, or smart-contract controls (including pauses), and includes any functionally equivalent measure, however described.

Reconciliation of reserve account

75. (1) An issuer shall implement systems and controls to ensure that the number of issued stablecoins is continuously reconciled against the value and availability of corresponding reserve assets.

(2) Reserve accounts shall be reconciled on a daily basis with internal recordkeeping systems capable of real-time balance tracking.

Risk-based reserve management

76. (1) Issuers shall adopt and implement a written reserve management policy that includes—

(a) procedures for mitigating liquidity risks, including stress testing under adverse scenarios;

(b) controls for market risk, including market-to-market valuation of assets;

(c) systems for managing operational risk, including cybersecurity protocols; and

(d) systems for assessing, monitoring and managing stablecoin activities performed by third parties.

(2) The policy referred to in subsection (1) shall be reviewed and updated annually, at a minimum.

Phased reserve benchmarks for stablecoin issuance

77. (1) Issuers shall adhere to the three-phase prudential reserve benchmarks applicable to its stablecoin issuance or as otherwise prescribed by the Commission, including—

(a) Phase 1: Full (1:1) reserve backing with no interest-bearing instruments permitted in the reserve;

(b) Phase 2: Full (1:1) reserve backing permitted with interest-bearing reserve instruments approved by the Commission; and

(c) Phase 3: Partial reserve backing with mandatory enhanced prudential oversight, systemic risk buffers and liquidity requirements permitted with the approval of the Commission.

(2) Progression between phases is subject to Commission approval based on systemic risk assessments, market maturity, and issuer compliance history.

(3) The Commission may determine the applicable phase for a licensed stablecoin issuer having regard to the nature, scale, complexity and risk profile of the stablecoin arrangement.

Tiered reserve requirements

78. (1) Issuers shall be subject to the minimum prudential, capital buffer and reserve requirements set out in Schedule 7.

(2) Tier 1 issuers must—

(a) hold one hundred percent (100%) reserve backing in high-quality liquid assets;

(b) have a minimum of specified reserve assets or USD 10 million (or currency equivalents) as a capital buffer;

(c) segregate user accounts;

(d) submit reserve attestation reports to the Commission monthly;

(e) conduct bi-annual financial audits; and

(f) make real time-time (24/7) reserve holdings disclosures that reflect current reserve composition, location and custodial arrangements publicly available in a format approved by the Commission.

(3) Tier 2 issuers must—

(a) hold one hundred percent (100%) reserve backing in high-quality liquid assets;

(b) have a minimum of specified reserve assets or USD 2 million (or currency equivalents) as a capital buffer; and

(c) conduct bi-annual financial audits and risk management reporting.

(4) Tier 3 issuers must—

(a) hold a minimum 80% backing in high-quality liquid assets with cash equivalent; and

(b) have USD100,000 (or currency equivalents) minimum paid-up capital.

(5) Tier 0 issuers—

(a) have no reserve requirement but are subject to mandatory disclosures based on prudential requirements; and

(b) redemption rights and restrictions must be approved by the Commission.

Reserve coverage minimums

79. (1) Issuers must maintain reserve assets equal to the outstanding value of issued stablecoins on at least a 1:1 basis.

(2) The Commission may prescribe a minimum threshold in monetary terms in addition to percentage-based requirements.

(3) Where stablecoins offer yield or involve complex risk structures, the Commission may require—

(a) reserve holdings in excess of one hundred percent (100%); or

(b) additional capital buffers and liquidity stress coverage.

Governance Disclosures

80. An issuer shall disclose to the Commission in the prescribed form and at the prescribed frequency—

(a) the governance framework for reserve management, including board-level responsibilities and delegated authorities;

(b) the composition and mandate of the risk and audit committees, including the frequency of meetings and the processes for reporting to the board; and

(c) the measures adopted to identify, manage, and disclose conflicts of interest, including related-party transactions involving reserves.

Regulatory Reporting

81. (1) Each issuer shall prepare and submit such reports, returns, and disclosures as may be required by the Commission under this Act or any other applicable law.

(2) Issuers shall submit to the Commission, in the prescribed form and frequency—

(a) a breakdown of reserve asset composition by type, value, location, and

(b) custodial institution;

(c) redemption performance and outstanding liabilities;

(c) results of liquidity and stress testing exercises; and

(d) any material changes in risk management policy or governance structure.

(3) The Commission may issue rules, guidelines, or directives specifying the scope of reporting obligations, including—

(a) reserve composition and valuation;

(b) transactional volumes and redemption activity;

(c) risk exposure metrics and liquidity positions; and

(d) any material events or changes affecting the stablecoin activities of the issuer.

(4) Issuers shall comply with all other international regulatory reporting obligations under this Act or any other Act, as appropriate.

Public disclosures and reporting

82. (1) An issuer shall make such public disclosures as are necessary to ensure transparency, promote market integrity, and enable users to make informed decisions regarding stablecoin activities at least monthly on any publicly accessible website that it maintains or as otherwise approved by the Commission.

(2) An issuer shall maintain and publish up-to-date disclosures, in a format approved by the Commission, including—

(a) valuations, custodianship arrangements, maturity profiles and location of reserve assets, ensuring interoperability with regulatory and public monitoring requirements;

(b) its stablecoin redemption policies and liquidity framework, including—

(i) if redemptions are not guaranteed at par; and

(ii) conditions for redemptions (fees, processing times, minimum amounts.

(c) summaries of audit findings, including—

(i) auditor details (name, qualifications, etc.);

(ii) a statement by Issuer's management that reserves adequately support stablecoins in circulation;

(iii) examination scope and period covered;

(iv) detailed information on backing assets (types, amounts, valuation methods);

(v) custodial arrangements for safekeeping assets;

(vi) auditor's findings and opinion on reserve adequacy;

(vii) risk disclosures (e.g. de-pegging, liquidity risks);

(viii) date of any statements or attestation reports;

(ix) signatures from the auditor and Issuer management.

(d) notice of any material operational, legal or governance changes, including an updated White Paper detailing—

(i) business description;

(ii) rights and obligations of stablecoin holders; and

(iii) risks affecting stablecoin stability and issuer obligations.

(e) its investment policy and backing assets, including types, issuers, and target credit ratings;

(f) information to clients on—

(i) stablecoins in circulation;

(ii) composition and market value of backing assets; and

(iii) data updated monthly or upon client request (not older than thirty (30) days).

(g) Risk Overview including—

(i) business activities and associated risks;

(ii) risk management policies; and

(iii) current and emerging risks.

(3) The information referred to in subsection (1) shall be presented in a clear and comprehensible manner, in accordance with standards prescribed by the Commission.

(4) Issuers shall publish periodic reserve asset disclosures in a machine-readable format which shall detail asset composition, valuation methodologies, custodianship, and maturity structure.

(5) Issuers shall conduct and publicly disclose the results of periodic stress tests evaluating the adequacy, liquidity, and resilience of reserve assets under simulated adverse market conditions in structured data formats and explanatory methodologies.

(6) All customers of Issuers shall receive a regulatory-approved risk disclosure statement at onboarding and at regular intervals, summarising redemption rights, reserve composition, custodial risks, and governance practices.

(7) The structure of the White Paper as set out in Schedule 3 may serve as a model for the White Paper and user disclosure obligations as prescribed by the Commission.

(8) The issuer shall submit periodic reports to the Commission, in the prescribed form and frequency, including—

(a) breakdown of reserve composition by type, value, location and custodian;

(b) outstanding liabilities and issuance/redemption flows;

(c) results of liquidity and stress testing; and

(d) material changes in governance, risk policy or technology.

(9) The Commission may require Tier 1 issuers to provide real-time (24/7) public disclosures of reserve holdings and composition, and may prescribe the method and safeguards for such disclosures.

Independent attestation and audit

83. (1) An issuer shall appoint an independent auditor approved by the Commission.

(2) The issuer shall obtain independent assurance, at a frequency prescribed by the Commission, verifying—

(a) sufficiency and composition of reserves;

(b) adherence to liquidity and solvency requirements;

(c) effectiveness of reserve controls and risk management

(d) reconciliation processes and controls; and

(e) redemption operations and stress testing results.;

(3) Audit or attestation reports shall be submitted to the Commission within the prescribed period and may be required to be made publicly available, subject to the Commission's directions.

Governance and risk management

84. (1) An issuer shall establish a governance framework that provide effective oversight of the stablecoin arrangement, including clear accountability for reserve management, redemption operations, technology risk and compliance.

(2) The issuer shall maintain policies for—

(a) reserve investment, valuation and liquidity management;

(b) stress testing and contingency planning;

(c) conflicts of interest and related-party exposures; and

(d) operational resilience and outsourcing.

(3) The Commission may impose additional prudential obligations for Tier 1 or Tier 2 issuers, including additional capital buffers.

Governance disclosures for reserve management

85. (1) An issuer shall disclose to the Commission in the prescribed form and at the prescribed frequency—

(a) the governance framework for reserve management, including board-level responsibilities and delegated authorities;

(b) the composition and mandate of the risk and audit committees, including the frequency of meetings and the processes for reporting to the board; and

(c) the measures adopted to identify, manage, and disclose conflicts of interest, including related-party transactions involving reserves.

(2) In the case of a stablecoin governed by a DAO, an Issuer must—

(a) publish on a public, accessible medium—

(i) governance rules and voting mechanisms;

(ii) upgrade and change management procedures; and

(iii) allocation and use of treasury funds.

(b) implement and disclose—

(i) multi-party authorisation (M-of-N) for key protocol functions;

(ii) independent third-party review of smart contracts; and

(iii) identification of key signatories and voting power distribution.

(3) Where the DAO's governance affects the stability, security, or redemption of the stablecoin, such governance structure shall be subject to oversight and enforcement actions by the Commission.

(4) The Commission may prescribe additional requirements in relation to the form and timing of such disclosures as it considers appropriate.

(5) Where failure to establish adequate internal systems, governance, training, or controls materially contributes to breaches under this Act, executive officers, board members, or controlling persons may be held personally liable in accordance with applicable law, regardless of whether direct intent or gross negligence is proven.

Technology and operational resilience for stablecoin arrangements

86. (1) As prescribed by Part 7, an issuer shall ensure that any smart contracts or critical on-chain components are subject to independent security audits and ongoing monitoring.

(2) The issuer shall maintain robust key management, access control, change management, and incident response capabilities.

(3) The Commission may prescribe additional requirements for systemic stablecoin arrangements, including recovery and resolution planning.

Restrictions and prudential measures

87. (1) The Commission may impose restrictions on stablecoin activities where it considers it necessary for financial stability, consumer protection or market integrity, including restrictions on—

(a) the use of particular stabilisation mechanisms;

(b) offering yield or profit-sharing features;

(c) composition or concentration of reserve assets; and

(d) cross-border distribution.

(2) The Commission may prescribe tiered reserve requirements, capital buffers and prudential standards, including—

(a) Tier 1 issuers: one hundred percent (100%) reserve backing in high-quality liquid assets and a minimum capital buffer of [USD 10 million] (or currency

equivalent); monthly reserve attestations; bi-annual audits; and real-time reserve disclosures;

(b) Tier 2 issuers: one hundred percent (100%) reserve backing in high-quality liquid assets and a minimum capital buffer of [USD 2 million] (or currency equivalent); and bi-annual audits and risk reporting;

(c) Tier 3 issuers: a minimum eighty percent (80%) backing in high-quality liquid assets plus cash equivalents and minimum paid-up capital of [USD 100,000] (or currency equivalent); and

(d) Tier 0 issuers: no reserve requirement, but mandatory prudential disclosures and Commission-approved redemption rights and restrictions.

(3) In addition to subsection (1) and (2), the Commission may require reserve holdings in excess of one hundred percent (100%) or additional capital buffers for stablecoins that offer yield or involve complex risk structures.

Transitional provisions for stablecoins

88. (1) This section applies separately from section 103 having regard to the distinct prudential, reserve management, redemption and customer protection considerations applicable to stablecoin activities.

(2) In compliance with Section 103, a person carrying on stablecoin activities immediately before the commencement of this Part must, within the prescribed period, apply for the authorisation or cease the activity.

(3) During the transitional period, the Commission may impose interim conditions, including restrictions on new issuance, to protect users and market integrity.

(4) The Commission may issue transitional directions for migration to full compliance, including tier determination and phased implementation of reporting and disclosure requirements under Sections 80 to 83.

PART X

CUSTOMER AND USER PROTECTION

Rights and Protections for virtual asset customer and user

89. (1) Each VASP shall conduct virtual asset activities in a manner that ensures the fair, transparent, and prudent treatment of customer and user of virtual assets, and shall implement appropriate measures to safeguard customer and user rights, interests, and funds.

(2) VASPs shall provide clear, accurate, and fair disclosures to customers as prescribed, including—

(a) associated risks, including potential de-pegging, insolvency, and liquidity constraints;

(b) redemption rights, specifying the process, fees, and timeframes for converting virtual assets back to fiat;

(c) terms of use, including dispute resolution mechanisms for users;

(d) reserve composition and the safeguards in place to protect customer funds;

(e) contribution to public financial education initiatives on digital asset risks, to be coordinated by the Commission annually; and

(f) any other disclosure that the Commission may consider necessary.

(3) Users shall have access to—

(a) fair and transparent fees with no hidden charges;

(b) timely and accessible customer support for transaction-related issues; and

(c) a dispute resolution process in case of misconduct by VASPs.

(4) A licensed VASP shall not, in trade or commerce, engage in conduct that is misleading or deceptive or is likely to mislead or deceive a customer or user.

(5) A licensed VASP shall not engage in unconscionable conduct in connection with the supply of virtual asset services.

(6) A term of a consumer contract is void if the term is unfair, having regard to—

(a) whether it causes a significant imbalance in the parties' rights and obligations;

(b) whether it is reasonably necessary to protect the legitimate interests of the VASP; or

(c) whether it would cause detriment to a customer if relied upon.

(7) The Commission may issue regulations prescribing unfair contract terms, mandatory disclosures, cooling-off rights and retail participation safeguards.

Fraud Prevention and Redress Mechanisms

90. (1) A VASP shall implement and maintain effective systems, controls, and procedures to detect, prevent, and respond to fraudulent or abusive conduct in connection with virtual asset activities.

(2) VASPs shall implement fraud detection mechanisms, including—

(a) transaction monitoring to detect abnormal or suspicious patterns;

(b) on-chain fraud detection tools to track illicit activities;

(c) real-time alerts for high-risk transactions, such as large withdrawals or cross-border movements;

(d) establish and publicise clear processes for lodging complaints or claims related to fraud or unauthorised transactions; and

(e) provide timely investigation, resolution, and redress in accordance with standards prescribed by the Commission.

(3) A VASP shall take reasonable steps to prevent scams, fraud, market manipulation and misleading promotional practices.

(4) A VASP shall implement enhanced consumer risk warnings in a format prescribed by the Commission.

Customer Redress Mechanisms

91. (1) The Commission may establish or designate a compensation fund or other mechanism to ensure that customers or eligible users who suffer financial loss arising from fraud, mismanagement, or insolvency of a licensed entity to have timely and effective to access to compensation.

(2) Contributions to a fund may be required from VASPs, based on criteria prescribed by the Commission, including—

(a) volume of issued virtual assets;

(b) level of user assets held; and

(c) systemic risk designation or compliance history.

(3) Customers shall have the right to file complaints with the Commission, which shall investigate cases in a timely manner.

(4) A VASP shall have virtual asset recovery and resolution procedures available in cases of unauthorised transactions or system failures**.**

(5) Without limiting any other remedy, a customer who suffers loss as a result of contravention of this Part may bring a civil action for damages, rescission, or other relief.

(6) The Court may grant injunctions, restitution orders, compensation orders or other appropriate remedies.

PART XI

SUPERVISION

Investigations, examinations and inspections

92. (1) All VASPs issuing or offering initial virtual asset offerings in accordance with Part 3, shall be—

(a) subject to investigation or examination by the Commission at any time or in any way deemed necessary by the Commission for the purposes of exercising its powers, performing its functions or

fulfilling its objectives under this Act and AML/CFT/CPF requirements;

(b) Subject to Section 11, VASPs are required to co-operate with the Commission during any investigation or examination; and

(c) required to provide the Commission with any information requested by the Commission to facilitate any investigation or examination.

(2) The Commission may conduct off-site monitoring and on-site inspections of a VASP, and may require production of records and information.

(3) For the purposes of an inspection or investigation, an authorised officer may—

(a) enter, at reasonable times, the business premises of a VASP or any person reasonably believed to hold relevant records;

(b) inspect and copy records, data and systems;

(c) require a person to provide explanations and assistance; and

(d) require access to systems, including through secure remote access where appropriate.

(4) The Commission may apply to the Court for a warrant where entry is refused or where the Commission considers a warrant necessary.

(5) A person who obstructs the Commission or an authorised officer commits an offence and is liable on conviction to the penalties prescribed in Section 99.

PART XII

ENFORCEMENT AND APPEALS

Directions and remedial powers

93. (1) Where the Commission considers that a VASP has contravened this Act or that a VASP's conduct poses a risk to customers or market integrity, the Commission may issue a written direction requiring the VASP to—

(a) take specified remedial action;

(b) cease or restrict specified activities;

(c) replace or remove a director, senior officer or key function holder, subject to due process;

(d) commission an independent review and implement recommendations; or

(e) implement enhanced controls or safeguards.

(2) A VASP shall comply with a direction within the time specified.

(3) Failure to comply with a direction is liable to administrative or supervisory action under Section 94.

Administrative and supervisory penalties (non-compliance)

94. (1) Where the Commission is satisfied that a VASP, stablecoin issuer or any other person subject to this Act has contravened this Act, regulations, rules, codes or licence conditions, the Commission may impose one or more administrative penalties.

(2) Administrative penalties may include—

(a) written warning or reprimand;

(b) public censure;

(c) administrative fine not exceeding the prescribed amount;

(d) variation or imposition of licence conditions;

(e) suspension of activities;

(f) restriction on new business; or

(g) any other remedial measure as prescribed by Regulations.

(3) Before imposing an administrative penalty, the Commission shall give notice and an opportunity to be heard, unless urgent action is necessary.

(4) An administrative penalty under this Section does not preclude a person from criminal proceedings or sanctions prescribed in Sections 98 and 99.

Injunctions and court orders

95. (1) The Commission may apply to the Court for an injunction or other order where it considers it necessary to—

(a) restrain a contravention of this Act;

(b) compel compliance with this Act or a direction;

(c) protect customer assets or reserve assets; or

(d) prevent market abuse or fraud.

(2) The Court may make such orders as it considers just, including interim orders.

Freezing and preservation orders

96. (1) Where the Commission reasonably suspects that a person is carrying on unlicensed virtual asset business or that customer assets or reserve assets are at risk, the Commission may apply to the Court for an order—

(a) freezing assets or restricting dealings;

(b) appointing a receiver or administrator; and

(c) requiring the preservation of records and data.

(2) The Court may make such orders as it considers necessary for the protection of customers and the public.

Winding-up and insolvency-related powers

97. (1) Where a VASP is insolvent or is likely to become insolvent, or where it is in the public interest, the Commission may apply to the Court for the winding-up of the VASP or for the appointment of an administrator or receiver in accordance with the Companies Act.

(2) In proceedings under subsection (1), the Court shall have regard to the need to protect customer assets and to facilitate orderly return of customer assets and reserve assets.

(3) The Commission may issue directions to a VASP in financial distress regarding cessation of business, communication to customers, and safeguarding of assets.

General offences

98. (1) A person commits an offence where that person—

(a) carries on virtual asset business without a licence in contravention of Section 13;

(b) carries on stablecoin activities without authorisation under Part 9;

(c) knowingly provides false or misleading information to the Commission;

(d) obstructs or fails to comply with a lawful requirement of the Commission; or

(e) contravenes any provision of this Act expressly stated to constitute an offence.

(2) Where an offence under this Act is committed by a body corporate, every director, officer or person concerned in the management who knowingly authorised or permitted the commission of the offence also commits an offence.

Sanctions by the Court upon Conviction

99. (1) A person convicted of an offence under this Act is liable—

(a) on summary conviction, to a fine not exceeding $50,000 or imprisonment for a term not exceeding 12 months, or both;

(b) on conviction on indictment, to a fine not exceeding $250,000 or imprisonment for a term not exceeding 4 years, or both.

(2) In addition to any penalty imposed under subsection (1), the Court may—

(a) order restitution to affected customers;

(b) disqualify a person from acting as a director or controller of a VASP;

(c) order confiscation of proceeds under POCA; or

(d) make any ancillary order necessary to give effect to this Act.

Appeals

100. (1) A person who is aggrieved by a decision of the Commission under this Act may appeal in accordance with the procedure as prescribed by Regulations, or where none is prescribed, to the Supreme Court within thirty (30) days of notice of the decision.

(2) An appeal under this Section shall be made to the Supreme Court within the time and in the manner prescribed under the FSCA, and the filing of an appeal shall not operate as a stay of the decision appealed from unless the Court otherwise orders.

(3) An appeal does not operate as a stay of the decision unless the Court orders otherwise.

PART XII

MISCELLANEOUS

Regulations, rules and guidance

101. (1) Notwithstanding the specific obligations imposed by this Act, the Commission may issue such supplementary rules, guidelines, regulatory circulars, protocols, codes of practice, or binding directions as may be necessary to give full effect to the provisions of this Act or to provide for its proper administration, supervision, and enforcement..

(2) Without limiting the generality of subsection (1), such rules, guidelines, circulars, protocols, codes or directions may include provisions relating to the general administration, regulation and implementation of the virtual asset regulatory framework in the Islands**.**

(3) The Governor may make regulations for carrying into effect the provisions of this Act, including—

(a) licence classes, application processes, fees and forms;

(b) capital, liquidity, insurance and prudential requirements;

(c) customer asset safeguarding standards;

(d) technology and cybersecurity standards;

(e) travel rule requirements and technical standards;

(f) stablecoin tier thresholds and reserve asset eligibility;

(g) administrative penalties and enforcement processes; and

(h) transitional provisions and commencement sequencing.

(4) A regulation or rule may create offences punishable on summary conviction by a fine not exceeding $25,000.

Fees

102. (1) The Govenor may prescribed by regulation fees and penalties in respect of, among other things, applications, licences, approvals, renewals, approvals, inspections and supervision, as appropriate.

(2) Fees may be risk-based and may reflect the complexity and scale of a VASP's activities.

(3) The prescribed fees and penalties shall be payable to the Commission or Registrar, as appropriate.

(4) Unless this Act or regulations provide otherwise, an authorised person is the only person able to pay a fee or penalty to the Registrar under this Section, and the Commission or Registrar shall not accept a fee or penalty paid by any other person.

(5) The Registrar may refuse to take any action required of him under this Act for which a fee is prescribed until all fees and penalties have been paid.

(6) The Governor may prescribe by regulations supervisory fees payable by licensees based on risk class, gross revenue, volume of activity or such other objective criteria as may be specified, and may cap or tier such fees.

(7) The Governor may waive or modify prescribed fees from time to time as appropriate.

Transitional and savings

103. (1) A person who, immediately before commencement of this Act, was carrying on virtual asset business in or from within the Islands may continue to carry on that business during a transitional period of ninety (90) days after commencement, if the person submits, within that period, an application for interim registration in the form and manner prescribed by the Commission.

(2) On receiving an application under subsection (1), the Commission may grant interim registration subject to conditions and may permit the applicant to continue to carry on VASP business for such further period as the Commission may specify (not exceeding 6 months), or until the application for authorisation is determined, whichever occurs first.

(3) A person who fails to apply within the period in subsection (1), or whose interim registration is refused, revoked or expires, shall immediately cease carrying on VASP business and shall comply with any wind-up directions issued by the Commission.

(4) A person who fails to submit an application as prescribed in subsection (1) commits and offence.

Amendment of Schedules

104. (1) The Governor may, by Regulations made under this Act, amend any Schedule to this Act, and such Regulation shall be subject to negative resolution.

(2) An order made under this Section shall be laid before Parliament at its next meeting immediately following the date of publication of the order in the Gazette.

(3) If, at the meeting of Parliament referred to in subsection (2), Parliament passes a resolution annulling an order which has been laid before it in accordance with that subsection or if an order made under this Section is not laid before Parliament in accordance with that subsection, that order shall cease to have effect on and after the day of the annulment or the day next following the day that the meeting is concluded, as the case may require, but without affecting the validity or curing the invalidity of anything done or omitted to be done thereunder before that day or the making of a new order.

(4) Notwithstanding section 23(2) of the Interpretation Act, where—

(a) an order is annulled under subsection (3) or is not laid before Parliament in accordance with subsection (2); and

(b) that order amended or revoked an order that was in operation immediately before the first mentioned order came into operation,

the annulment or failure to comply with subsection (2) revives the previous order on and after the day of the annulment or, in the case of failure to comply with subsection (2), on and after the day next following the day that the meeting of Parliament referred to in subsection (2) is concluded.

Review of Act

105. (1) The Commission may, within three (3) years of commencement, cause a review of the operation of this Act to be undertaken and submit a report to the Governor.

(2) The review shall consider effectiveness, proportionality, and alignment with international standards.

Binding on the Crown

106. This Act binds the Crown.

SCHEDULE 1

MINIMUM CRITERIA FOR APPLICATIONS FOR VASP LICENCE

(Section 18)

Applications requirements

1. (1) VASPs who wish to conduct virtual asset business must comply with Section 17 application requirements in order to be licensed to conduct virtual asset activities as a business in the Islands—

(2) Corporate information: legal name, registration details, registered office, group structure chart, controllers and beneficial owners;

(3) Governance: directors, senior management, key function holders; roles and responsibilities; policies for fitness and propriety; remuneration and conflicts framework;

(4) Business plan: description of activities, products and services; target customers and jurisdictions; projected volumes; pricing and revenue model; outsourcing arrangement;

(5) Risk management: enterprise risk assessment; operational risk; market risk (where relevant); custody risk; third-party risk; fraud risk; and

(6) ML/FT/PF: business risk assessment; CDD processes; monitoring; sanctions screening; travel rule implementation; training plan; MLRO appointment.

SCHEDULE 2

MINIMUM CRITERIA FOR APPLICATIONS FOR STABLECOIN BUSINESS LICENCE

(Sections 18 and 65)

Minimum public disclosures (non-exhaustive) – internal policies:

2. (1) VASPs who seek to conduct stablecoin business as a VASP shall comply with Section 17 application requirements and the requirements as follows—

(a) stablecoin description, stabilisation mechanism and risks;

(b) redemption user rights, timelines, fees and terms and conditions;

(c) reserve asset eligible, custody, segregation, and investment limits;

(d) governance, risk management, and audit/attestation arrangements;

(e) incident reporting and operational resilience disclosures.

(f) technology architecture, smart contracts, audits and security controls;

(g) contingency plans, including recovery and wind-up; and

(h) proposed public disclosures and user communications.

SCHEDULE 3

LICENCE CLASSES AND PERMITTED ACTIVITIES

(Sections 12, 16 to 65)

Virtual Asset Business – Licence classifications

1. As prescribed, the Commission may grant one or more of the following classes of virtual asset business licence—

Classification	Permitted Virtual Asset Activity
Class A Virtual Asset Exchange	Provide the following class-specific information and supporting documents: -Market structure description (order types, matching, market surveillance). -Listing policy (admission, ongoing monitoring, delisting). -Client onboarding and disclosures; conflicts of interest policy. Safeguarding model (custody in-house / third party); reconciliation procedures. -Settlement model and fiat rails; bank/PSP letters of intent.
Class B – Custody and Wallet Services	Provide the following class-specific information and supporting documents: - Custody control framework; key management policy (HSM/MPC; key ceremony). -Segregation of client assets; reconciliation and proof-of-reserves approach. -Insurance arrangements (if any) and coverage summary. -Hot/warm/cold wallet structure; access controls and audit logs. -Outsourcing arrangements (if custody sub-contracted)
Class C – Transfer and Payment Services	Provide the following class-specific information and supporting documents: - Transfer rails and payment flow diagrams (VA and fiat). - Settlement finality and reconciliation methodology. - Safeguarding of fiat balances; escrow/trust account arrangements.

	-Fraud controls, chargeback/dispute handling (where applicable). -Sanctions screening and Travel Rule solution details.
Class D – Stablecoin Issuance / Issuer arrangements	Provide the following class-specific information and supporting documents: - Stablecoin design, backing/peg mechanism, issuance/redemption process. -Reserve policy; eligible reserve assets; custody/escrow arrangements. -Redemption policy and timelines; liquidity buffer plan. -Disclosure (White Paper/terms); consumer risk disclosures. -Independent assurance: attestation/audit plan and reporting cadence.
Class E– Trading Platform Operator	Provide the following class-specific information and supporting documents: - Platform design and rule book; participant eligibility and onboarding. -Market integrity controls (surveillance, abuse monitoring). -Order book / trading rules; transparency and reporting. -Custody/settlement interface and safeguarding controls. -Business continuity and operational resilience plan.

Classification of VASP licences

2. (1) The Commission may prescribe separate application fees for according to each classification of VASP licence—

(a) a full (perpetual) licence;

(b) a Sandbox (temporary) licence; and

(c) an extension of a Sandbox licence (where permitted).

3. (1) In accordance with its authority under Section 102, the Commission may prescribe how fees apply where an applicant seeks authorisation for more than one licence class.

(2) The Commission may specify, by rules, which classes may be combined and any additional conditions applicable to each class or category of licence, including capital, insurance and technology standards.

VASP Licence classification: minimum liquidity requirements

4. (1) The Commission may prescribe minimum liquidity and escrow requirements for each class of VASP licence—

Licence class	Minimum liquidity / escrow requirements
All classes (A–E)	Maintain at all times liquid financial resources sufficient to meet (i) 3 months of projected fixed operating expenses; and (ii) anticipated wind-up costs. Liquid resources shall be held in cash or cash equivalents with an eligible bank/custodian and shall be unencumbered.
Class A – Exchange / marketplace-facing models	Liquidity coverage ratio (LCR): Liquid Assets ≥ (Client Fiat Payables + 3 months fixed operating expenses). Where client fiat is held, it shall be held in segregated trust/escrow accounts. Daily reconciliation required.
Class B – Custody / wallet services	Operational liquidity: Liquid Assets ≥ 3 months fixed operating expenses. Client asset safeguarding: 100% segregation of client assets; key management controls; insurance (where available) commensurate with risk.
Class C – Transfer / payment services	Liquidity: Liquid Assets ≥ 2 months fixed operating expenses. If transmitting fiat or settling client balances, maintain settlement buffer and segregated accounts with daily reconciliation.
Class D – Stablecoin issuance / issuer arrangements (if permitted)	Reserve/escrow: 1:1 backing of 'specified stablecoin' liabilities by eligible reserve assets held in segregated custody/escrow accounts. Redemption liquidity: maintain a cash buffer to meet peak redemptions (minimum 10% of outstanding liabilities in cash or cash equivalents unless otherwise approved). Monthly reserve attestation; quarterly independent assurance.
Class E – Trading platform operator / order book	Liquidity: Liquid Assets ≥ 3 months fixed operating expenses. If interfacing with custody/settlement, comply with Class A/B safeguarding requirements as applicable.

SCHEDULE 4

INITIAL VIRTUAL ASSET OFFERINGS

(Part 6)

White Paper requirements

1. (1) A person shall not offer or 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) the beneficial owners of the VASP;

(iii) names the VASP 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 it is calculated, and when and to whom it is 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 shall 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; and

(b) notifies the Commission of its intention to make the virtual asset available to the public, where the total amount of virtual assets made available in the Islands exceeds [insert threshold amount].

(2) An issuer must—

(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 twelve (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; and

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

SCHEDULE 5

WHITE PAPER STRUCTURE

(Section 43)

Minimum requirements for White Paper Disclosures:

This guides issuers on the necessary content for user-facing White Papers—

(a) Executive Summary;

(b) Stablecoin Mechanism and Peg Details;

(c) Issuer Legal Entity and Governance;

(d) *R*eserve Composition and Safeguards;

(e) Redemption Process and User Right;

(f) Fees and Charges;

(g) Risk Disclosures (market, operational, cyber);

(h) Audit and Transparency Policies;

(i) Legal and Regulatory Disclaimers; and

(j) Contact Information and Complaints Handling.

SCHEDULE 6

TIERED LICENSING FRAMEWORK FOR STABLECOINS ISSUERS

(Section 67)

(1) Tiered classification of stablecoins under this Act

Tier	Criteria	Regulatory Obligations
Tier 1 – systemic stablecoins	- Widely used for payments or settlement - Market capitalization above [X threshold] - Significant cross-border usage	- Full prudential requirements - Reserve asset segregation - Daily reporting to regulator - Enhanced governance standards
Tier 2 – significant stablecoins	- Moderate market capitalization - Domestic usage with limited cross-border exposure - Backed by regulated custodians	- Capital and liquidity requirements - Monthly reporting - Independent audit annually
Tier 3 – limited-Use stablecoins	- Small-scale issuance - Restricted to closed-loop ecosystems (e.g. gaming, loyalty programmes) - Market capitalization below [Y threshold]	- Registration with regulator - Basic disclosure obligations - Consumer protection safeguards
Tier 0 (Sandbox)		

SCHEDULE 7

TIERED RESERVE REQUIREMENTS OF STABLECOINS ISSUERS

(Section 78)

(2) Minimum quantitative thresholds:

Tier	Market Capitalisation (USD or currency equivalents)	Active User Base	Average Daily Transaction Volume (USD)	Cross-Border Usage
Tier 0	≤ 5 million	≤ 10,000	≤ 100,000	Not permitted
Tier 3	≤ 5 million	≤ 10,000	≤ 500,000	Minimal
Tier 2	5 to 500 million	10,000 to 1 million	≤ 100 million	Moderate
Tier 1	> 500 million	> 1 million	> 100 million	Extensive

SCHEDULE 8

Turks and Caicos Islands Financial Services Commission
Guidance Note on Stablecoin Redemption and Convertibility

(Part 9)

Purpose and status of this Guidance Note

1. Issued under the stablecoin provisions under Part 9 of the Virtual Assets Business Act 2026

1.1 This Guidance Note is issued by the Turks and Caicos Islands Financial Services Commission ("the Commission") to provide regulatory guidance on the interpretation and application of Section 75 of Part 9 (Redemption and Convertibility) of the Act.

1.2 This Guidance Note does not have the force of law but sets out the Commission's supervisory expectations. Failure to have regard to this Guidance Note may be taken into account in the exercise of the Commission's supervisory, enforcement, and licensing powers.

Regulatory objective

2.1 The objective of the redemption framework is to ensure that stablecoins—

(a) remain reliably redeemable at par value;

(b) do not give rise to consumer detriment or market disorder; and

(c) are supported by sound liquidity, operational, and governance arrangements.

2.2 The Commission considers timely redemption to be a core prudential and consumer protection requirement.

Redemption settlement timing (T+1)

3.1 The Commission expects issuers to settle valid redemption requests no later than T+1, being the next business day following receipt of the request.

3.2 Issuers are encouraged to process redemptions on a same-day (T) basis where operationally feasible and where requests are received before published cut-off times.

3.3 T+1 is regarded as the maximum outer limit under normal operating conditions and not a target or standard settlement period.

Cut-off times

4.1 Issuers may apply cut-off times for same-day processing, provided such cut-off times are—

(a) clearly disclosed to holders;

(b) reasonable having regard to the issuer's operating model and settlement rails; and

(c) applied consistently and without discrimination.

4.2 Requests received after a cut-off time should be treated as received on the next business day for the purposes of calculating T and T+1.

Valid redemption requests

5.1 A redemption request is considered valid once the holder has—

(a) submitted the request through approved channels;

(b) satisfied applicable customer due diligence and verification requirements; and

(c) provided accurate and complete settlement instructions.

5.2 Issuers should not introduce unnecessary or duplicative steps that have the effect of discouraging or delaying redemption.

Liquidity and operational readiness

6.1 Issuers are expected to maintain sufficient high-quality liquid assets to meet foreseeable redemption demands, including during periods of stress.

6.2 Issuers should ensure that redemption processes are supported by—

(a) documented policies and procedures;

(b) clear internal escalation and exception handling; and

(c) business continuity and disaster recovery arrangements.

6.3 Liquidity stress testing should explicitly consider rapid or concentrated redemption scenarios.

Interaction with AML/CFT/CPF and sanctions obligations

7.1 The Commission recognises that redemption settlement may be delayed where necessary to comply with AML/CFT/CPF, sanctions, fraud prevention, or law enforcement obligations.

7.2 Any such delay should be—

(a) strictly limited to what is necessary;

(b) properly documented; and

(c) capable of supervisory review.

7.3 AML/CFT/CPF controls shall not be used as a de facto gating or liquidity management tool.

Suspension, restriction, and gating

8.1 Suspension or restriction of redemptions is expected to be exceptional and time-limited.

8.2 Issuers should not implement gating, queues, or pro rata settlement mechanisms unless—

(a) expressly permitted by the Commission; or

(b) directed by the Commission in the interests of holders or financial stability.

8.3 Any use of suspension or restriction mechanisms should be supported by—

(a) clear triggers;

(b) defined governance and approval processes; and

(c) transparent communication to holders.

Recordkeeping and audit trail

9.1 Issuers should maintain complete and accurate records of—

(a) redemption requests received;

(b) settlement timing and outcomes;

(c) delays and their causes; and

(d) communications with holders and the Commission.

9.2 Records should be sufficient to enable independent audit and supervisory assessment.

Supervisory engagement and reporting

10.1 Issuers shall notify the Commission promptly where—

(a) redemption settlement extends beyond T+1 for a material volume of requests;

(b) there are recurring delays or operational failures; or

(c) issues arise that may affect the issuer's ability to meet redemption obligations.

10.2 The Commission may require additional reporting, remediation plans, or independent assurance where concerns are identified.

Effective date

11.1 This Guidance Note takes effect on the date of issuance and applies to all stablecoin issuers licensed or authorised under the Act.

SCHEDULE 9

TIERED GOVERNANCE AND RISK REGULATORY REQUIREMENTS

(Section 68)

(3) Minimum Governance and Risk Control requirements:

Governance Element	Tier 3	Tier 2	Tier 1
Board Composition	Basic oversight	Non-executive board members	Independent majority
Risk Committees	Optional	Recommended	Mandatory
Internal Audit	Not required	Annual	Quarterly
Stress Testing	None	Annual	Biannual
Compliance Officer	Mandatory	Mandatory	Mandatory

SCHEDULE 10

TIERED TECHNOLOGY AND CYBERSECURITY REGULATORY REQUIREMENTS

(Sections 35, 47 and 76)

(4) Technology and Cybersecurity Requirements:

Tier 3	Tier 2	Tier 1	Tier 0
Annual cybersecurity self-assessment	Annual integrity audit and self-assessment	Annual cybersecurity audit, red-teaming	Sandbox security plan with no public access unless tested
Regulator-issued technical checklist	Business continuity test	24/7 SOC and real-time monitoring	

SCHEDULE 11

CYBERSECURITY ASSESSMENT

(Sections 47 and 50)

(5) Minimum requirements for Cybersecurity Assessment:

This sets out sample baseline expectations by which issuers shall conduct cybersecurity assessments, as follows—

(a) network security controls (firewalls, intrusion detection)

(b) access control and authentication mechanisms

(c) incident response and recovery procedures

(d) data encryption and secure storage

(e) periodic penetration testing and vulnerability scans

(f) SOC monitoring

(g) self-assessment reporting

SCHEDULE 12

FINANCIAL SYSTEM INTEGRATION AND CROSS-BORDER COMPATIBILITY

(Sections 10, 13, 52 and Part 12)

Cross-Border Recognition and Equivalence

1. (1) The Commission may recognise the regulatory and supervisory framework of a foreign country for virtual assets and VASPs as equivalent to the standards set out under this Act, provided that certain conditions are met, including—

(a) the foreign country demonstrates adherence to internationally accepted regulatory standards, including those promulgated by the international standard-setting bodies (FATF, FSB, BIS, and IOSCO);

(b) the regulatory regime ensures comparable levels of prudential, technological, and customer protection safeguards; and

(c) the foreign Commission maintains effective supervisory cooperation and information sharing arrangements with the Commission.

(2) Upon recognition of equivalence, Issuers licensed under that foreign regime may be granted a licence, exemption, or other regulatory relief in the Islands, subject to any conditions imposed by the Commission.

(3) The Commission shall maintain a public list of countries to be regarded as equivalent for the purposes of this Act, including any restrictions or conditions associated with such recognition.

(4) The Commission may withdraw or suspend the equivalence status of a Commonwealth member country where material changes occur in the legal, regulatory, or supervisory regime of the foreign Commonwealth member country that compromise the basis for recognition.

Cross-Border Cooperation and Information Sharing

2. (1) The Commission shall cooperate whether through information sharing, joint investigations, or supervisory coordination with—

(a) foreign financial regulators to ensure international compliance and prevent regulatory arbitrage;

(b) domestic law enforcement agencies and Financial Intelligence Units to detect and prevent financial crimes;

(c) International standard-setting bodies (e.g. FATF, IMF, BIS) to align with global best practices.

(2) Information sharing mechanisms shall be established for—

(a) cross-border AML/CFT/CPF investigations involving stablecoins;

(b) regulatory harmonisation to enable interoperability between countries;

(c) joint enforcement actions where entities operate across multiple countries.

Financial System Integration and Cross-border Compatibility

3. (1) A licensed issuer shall ensure that its systems, processes, and governance arrangements are designed to support interoperability with—

(a) domestic payment systems, financial institutions, and regulatory frameworks; and

(b) foreign payment networks, stablecoin regimes, and supervisory authorities, where applicable.

(2) Stablecoins shall be designed for seamless integration with financial institutions, central banks, and VASPs.

(3) Issuers shall ensure compliance with international financial messaging standards, including ISO 20022, to enable cross-border compatibility.

(4) Stablecoins shall support cross-chain interoperability mechanisms such as atomic swaps, bridge protocols, and inter-block communication standards.

(5) On-chain identity verification shall be integrated to meet regulatory requirements without compromising decentralisation.

SCHEDULE 13

SUPERVISION AND ENFORCEMENT FRAMEWORK

(GUIDANCE PRINCIPLES)

(Section 101)

(1) The Governor may make delegated legislation and, as appropriate, the Commission may make supplementary rules, guidelines, regulatory circulars, protocols, codes of practice, or binding directions as may be necessary to give full effect to the provisions of this Act or to provide for its proper administration, supervision, and enforcement including—

(a) prudential and conduct standards for yield-bearing stablecoins and real-world asset tokens, including licensing requirements, risk disclosures, asset segregation, product suitability, liquidity risk management, and capital adequacy frameworks;

(b) governance, audit, and reserve transparency requirements for algorithmic and DAO-issued stablecoins, including stress testing, failure scenarios, reserve composition disclosures, and automated stabilisation mechanisms;

(c) tiered classification criteria and associated obligations for issuers, based on activity scale, user base, financial exposure, or systemic importance;

(d) cross-border issuance, usage, and redemption of stablecoins, including interoperability protocols, regulatory passporting, and compliance with foreign country requirements;

(e) technology, information-security and cyber-resilience requirements, covering governance and baseline controls, secure consensus and secure software code practices, continuous threat monitoring, incident-response and business-continuity planning, as well as equivalent standards for critical third-party VASPs;

(f) anti-money laundering, counter-terrorism financing, and counter-proliferation financing obligations for stablecoin activities, consistent with international standards;

(g) complaint handling, dispute resolution, and customer protection mechanisms applicable to both issuers and VASPs;

(h) memoranda of understanding required for coordination between the Central Bank, Securities Regulator, Data Protection Authority and Financial Intelligence Unit;

(i) supervisory colleges, cross-border coordination mechanisms, and systemic risk monitoring frameworks and

(j) any matter necessary or incidental to the exercise of the functions of the Commission under this Act.

SCHEDULE 14

CONSEQUENTIAL AMENDMENTS

(Section 103)

This Schedule sets out recommended consequential amendments to other legislation in the Islands to ensure the Virtual Assets Business Act, 2026 (the "Act") can be implemented effectively, and that the Commission can supervise, regulate and enforce the regime coherently across AML/CFT/CPF, corporate, and relevant financial services perimeters.

Consequential amendments include—

Financial Services Commission Act CAP. 16.01) are amended by adding—

1. Virtual Assets Business Act, 2026 to the list under Part II of the Schedule of the FSCA (Prescribed Financial Services Acts) Regulations, ensuring VASPs are treated as "financial businesses" subject to AML/CFT/CPF legislation, regulated and supervised by the Commission and reporting to the Financial Intelligence Agency—

Proposed amendments:

(a) Section 2 – Interpretation: insert the following definition in alphabetical order—

"Virtual Assets Business Act, 2026" means the Virtual Assets Business Act, 2026.

(b) Section 4 – Functions of the Commission: insert a new paragraph after the existing paragraph dealing with regulation of financial services (typically after securities / insurance)—

"(h) to act as the competent authority for the regulation, licensing, supervision and enforcement of virtual asset service providers and virtual asset activities under the Virtual Assets Business Act, 2026."

Rationale: Section 4 is where every sectoral mandate of the Commission is enumerated. This mirrors how banking, insurance and securities powers are conferred.

Proceeds of Crime Act (CAP. 3.15) and AML/CFT/CPF Regulations and Code are amended to —

2. Explicitly map VASPs (and, where relevant, stablecoin issuers) into the AML/CFT/CPF perimeter and operationalise FATF Recommendations 15 and 16 compliance with "travel rule" obligations for virtual asset transfers by—

(a) including VASPs and, if in-scope, stablecoin issuers as "financial business" / "relevant person" categories (or the equivalent statutory list) for AML/CFT/CPF obligations;

(b) inserting an express cross-reference recognising travel rule obligations for "transfers of virtual assets", including any de minimis threshold adopted in the Act or subordinate instruments;

(c) confirming that suspicious transaction reporting (STR) and tipping-off provisions apply to VASPs (and stablecoin issuers where applicable).

(d) ensuring sanctions screening, targeted financial sanctions, and high-risk jurisdiction countermeasures expressly apply to VASPs (and stablecoin issuers where applicable); and

(e) ensuring that VASPs are subject to the same robust AML/CFT/CPF standards as other financial institutions and designated non-financial businesses and professions.

Proposed amendment: Insert a new paragraph in Schedule 2 (numbered consecutively)—

"Virtual asset service providers licensed or required to be licensed under the Virtual Assets Business Act, 2026."

Rationale: Schedule 2 is what triggers AML/CFT supervision. This is exactly how money services businesses, securities dealers, etc., are captured.

Anti-Money Laundering and Prevention of Terrorist Financing Regulations 2010, and any Code or Guidance issued under CAP. 3.15, are amended—

3. (1) *(a)* to include VASPs within the scope of supervised persons; and

(b) to provide for "travel rule" information requirements for qualifying virtual asset transfers and recordkeeping standards consistent with FATF Recommendation 16 (as applied to virtual assets transfers).

Proposed amendments:

(a) Interpretation: insert—

"virtual asset" and "virtual asset service provider" have the meanings given in the Virtual Assets Business Act, 2026.

(b) Application of AML obligations: insert a clarifying provision:

"The obligations under these Regulations apply to virtual asset service providers and virtual asset activities regulated under the Virtual Assets Business Act, 2026, including customer due diligence, record-keeping, suspicious transaction reporting, and sanctions compliance."

Rationale: It imports AML obligations automatically without re-engineering the Regulations.

Companies Act (CAP. 16.08) and any related registry practices are amended, as necessary, to support—

4. (1) local incorporation or licensing of foreign VASPs;

(2) disclosure and updating of beneficial ownership information for such entities, consistent with applicable beneficial ownership requirements; and

(3) align customer asset protections, segregation, and orderly wind-up expectations with insolvency outcomes for licensed entities.

Proposed amendment: insert a new subsection:

"A company shall not carry on virtual asset business within the meaning of the Virtual Assets Business Act, 2026, unless it is duly licensed or authorised under that Act."

Rationale: This aligns company law with financial services laws and prevents the argument that incorporation alone permits VA activity.

Banking Act / Insurance Act / payments-related legislation (as applicable) are amended—

5. To operationalise the "relationship with other laws" approach by adding clear cross-references and cooperation pathways for mixed-activity groups and adjacent perimeters—

(a) insert cooperation gateways enabling the Commission to exchange information (and coordinate supervision) where a group or activity intersects with banking, insurance, or payment instrument perimeters connected to virtual assets or stablecoins;

(b) clarify treatment of mixed-activity groups: where a group contains a bank/insurer/payment entity and a VASP (or stablecoin issuer), enable consolidated supervisory coordination and group-wide risk management programme alignment.

Investment Dealers (Licensing) Act (CAP. 16.13) and Mutual Funds Act (CAP. 16.07) are amended—

6. To avoid perimeter gaps and clarify that where a token constitutes a security or derivative, the securities perimeter applies and compliance is not displaced by the virtual assets regime—

(a) insert definitions and cross-references for "virtual asset", "security token" (if used), "virtual asset activity", and the Act;

(b) insert a perimeter clarification clause confirming that where a token constitutes a security/derivative or otherwise falls within the securities perimeter, the relevant securities legislation applies in addition to (and not in substitution for) obligations under the Act;

(c) provide explicit authority for the Commission to require a classification opinion/determination and supporting documentation where classification is necessary to determine the applicable perimeter bank/insurer/payment entity and a VASP (or stablecoin issuer), enable consolidated supervisory coordination and group-wide risk management programme alignment.

Proposed amendment: Insert:

"Where a virtual asset represents an interest in a collective investment scheme or mutual fund, that asset and any related activity remain subject to this Act notwithstanding its treatment under the Virtual Assets Business Act, 2026."

Rationale: This avoids tokenised fund interests slipping out of funds regulation.

7. Transitional savings for the Consequential Amendments Schedule
(not in the individual Acts).

Proposed wording:

"Any licence, approval or regulatory action lawfully taken by the Commission prior to the commencement of the Virtual Assets Business Act, 2026, in respect of an activity that would constitute virtual asset business under that Act, is taken to have been granted or taken under the corresponding provisions of that Act."

SCHEDULE 15

REGULATORY SANDBOX FRAMEWORK AND OPERATING REQUIREMENTS

(Part 8)

Interpretation and application

1. (1) In this Schedule—

(a) "sandbox" means the controlled, time-limited regulatory environment established by the Commission under Section 54;

(b) "sandbox authorisation" means an authorisation granted by the Commission under Section 55;

(c) "sandbox participant" means a person holding a sandbox authorisation;

(d) "testing plan" means a plan approved by the Commission in accordance with paragraph 4 and Annex B.

(2) This Schedule forms part of the conditions of a sandbox authorisation granted under Section 55.

(3) Nothing in this Schedule limits obligations under AML/CFT/CPF, sanctions, consumer protection, data protection or other applicable laws.

Eligibility for admission

2. (1) The Commission may grant a sandbox authorisation where it is satisfied that—

(a) the proposed activity is innovative;

(b) the regulatory treatment of the activity is uncertain or requires live testing;

(c) the applicant has adequate financial, technical and human resources;

(d) the applicant and its controllers are fit and proper;

(e) risks can be mitigated to an acceptable level; and

(f) there is a credible pathway to licensing or orderly exit.

(2) The Commission may refuse admission where testing would expose customers or the financial system to unacceptable risk.

Application requirements

3. (1) An application for sandbox authorisation shall include—

(a) corporate and ownership information;

(b) details of directors and key persons;

(c) description of the proposed activity and customers;

(d) a testing plan in accordance with paragraph 4;

(e) a risk assessment;

(f) customer disclosures including Annex A;

(g) safeguarding and custody arrangements; and

(h) an exit and wind-up plan.

(2) The Commission may require additional information or independent assurance.

Testing plan

4. (1) A sandbox participant shall comply with an approved testing plan.

(2) The testing plan shall specify—

(a) objectives and success criteria;

(b) duration and milestones;

(c) customer eligibility;

(d) limits under paragraph 5;

(e) custody and key management;

(f) cyber and operational resilience;

(g) AML/CFT/CPF controls;

(h) reporting under paragraph 10; and

(i) exit triggers.

(3) Material deviation from the testing plan requires prior Commission approval.

Limits and conditions

5. (1) The Commission may impose limits on customers, volumes, exposures, products, jurisdictions and marketing.

(2) Sandbox participants shall maintain controls to ensure compliance with all limits.

Customer protection

6. (1) Communications shall be fair, clear and not misleading.

(2) Mandatory sandbox disclosure shall be provided in the form set out in Annex A.

(3) A complaints handling and escalation process shall be maintained.

(4) The Commission may restrict retail participation or require enhanced safeguards.

Safeguarding and custody

7. (1) Customer assets shall be segregated and reconciled at least weekly.

(2) Secure key management, audit trails and authorisation controls shall be maintained.

(3) Independent assurance may be required by the Commission.

AML/CFT/CPF and sanctions

8. (1) Sandbox participation does not waive AML/CFT/CPF or sanctions obligations.

(2) Appropriate CDD, monitoring, reporting and recordkeeping shall be maintained.

Technology and incident notification

9. (1) Proportionate ICT and cybersecurity controls shall be maintained.

(2) Material incidents shall be notified promptly to the Commission.

Reporting and evaluation

10. (1) Baseline, periodic and final reports shall be submitted.

(2) Reports shall address compliance, incidents, complaints and testing outcomes.

Duration, extension and variation

11. (1) Sandbox authorisation is time-limited.

(2) The Commission may extend or vary conditions where appropriate.

Exit and wind-up

12. (1) A Commission-approved exit plan shall be maintained.

(2) Customer notification and asset return or transfer shall be completed on exit.

Suspension and termination

13. (1) The Commission may suspend or terminate a sandbox authorisation under Section 56.

(2) Directions issued by the Commission shall be complied with.

ANNEX A

MANDATORY SANDBOX CUSTOMER DISCLOSURE

Regulatory Sandbox Notice (Turks and Caicos Islands)

This service is operating under a Regulatory Sandbox authorisation granted by the Commission under the Virtual Assets Business Act, 2026.

The service is authorised for testing purposes only, for a limited period and within defined limits. Sandbox authorisation is not a full licence. The Commission does not guarantee the performance of the service or the value of any virtual asset.

Testing may be discontinued at any time, and you may be required to cease use of the service. Any assets held will be returned or transferred in accordance with the approved exit plan and applicable law.

ANNEX B

SANDBOX TESTING PLAN TEMPLATE

The testing plan shall address governance, innovation rationale, scope, limits, customer protection, safeguarding, AML/CFT/CPF controls, technology resilience, reporting and exit arrangements.

The Testing Plan shall include—

1. Applicant and Governance
2. Innovation and Sandbox Rationale
3. Product and Service Description
4. Testing Objectives and Success Criteria
5. Testing Limits and Controls
6. Customer Protection Framework
7. Safeguarding and Custody Arrangements
8. AML/CFT/CPF Controls
9. Technology, Cybersecurity and Resilience
10. Reporting Plan
11. Exit and Transition Plan
12. Declarations and Undertakings

SCHEDULE 16

(Application Package)

TURKS AND CAICOS ISLANDS

FINANCIAL SERVICES COMMISSION VIRTUAL ASSESTS SERVICE PROVIDERS APPLICATION PACKAGE (LICENCE CLASSES A- E)

1. Purpose and how to use this package

This Application Pack sets out the forms, Schedules and checklists required to apply for a licence under the Virtual Assets Business Act 2026 (the "Act"). It is designed to align with Turks and Caicos Financial Services Commission (the Commission) standard application format used across other licensing regimes and is proportionate by licence class (A–E).

2. Licence classes (A–E)

Applicants must select the licence class(es) that match the licensable virtual asset activities they propose to carry on:

• Class A – Virtual Asset Exchange (Fiat-to-Virtual Asset): exchange between fiat currency and virtual assets; and Virtual Asset Exchange (Virtual Asset-to-Virtual Asset): exchange between one or more virtual assets..

• Class B – Custody and Wallet Services: safekeeping or administration of virtual assets or instruments enabling control over virtual assets.

• Class C – Virtual Asset Transfer and Payment Services: transfer of virtual assets on behalf of another person and related payment services.

• Class D – Stablecoin issuer arrangements.

• Class E – Trading Platform Operator: operation of a virtual asset trading platform, marketplace or order book.

3. What you must submit (overview)

Submit the following completed items, together with all supporting documents referenced in the checklists.

VA-1: Application Form (with Class Schedule(s) A–E attached)

VA-2: Personal Questionnaire (each director, controller, beneficial owner, senior officer, key person)

VA-3: AML/CFT/CPF Programme Schedule (including risk assessment and Travel Rule arrangements)

VA-4: Technology and Cybersecurity Schedule (architecture, key management, incident response, DR/BCP)

VA-5: Financial Resources, Liquidity and Safeguarding Schedule (including escrow arrangements)

VA-6: Declarations, Undertakings and Consent to Checks

4. Fees and payments (summary)

Fees are as prescribed by Regulations. A summary (USD) is set out below for convenience.

Licence class	Application fee	Grant / issuance fee	Annual supervisory fee
Class A (Virtual Asset Exchange)	7,500	20,000	20,000
Class B (Custody / Safekeeping / Wallet custody)	5,000	15,000	15,000
Class C (Broker/Dealer / Execution / Intermediation)	5,000	15,000	15,000
Class D (Stablecoin Issuance / Issuer arrangements)	10,000	25,000	25,000
Class E (Other VASP services)	3,750	12,500	12,500

Other application/event fees (USD):

Item	Fee (USD)
Application to vary licence conditions / business plan update requiring approval	1,500
Add an additional licence class to an existing licence (per class added)	2,500
Change of control approval application	2,500
Approval of new director / senior officer / key person (per person)	750
Approval of MLRO / Compliance Officer appointment (per role)	750
Approval of branch / new material outsourcing arrangement (per request)	1,000
Application for exemption / dispensation (per request)	1,000
Surrender / cancellation processing (where initiated by authorised person)	500

Supervisory and enforcement cost recovery (USD):

Item	Fee (USD)
Onsite inspection — daily rate (per inspector)	1,500
Special review / skilled person report — administration fee (plus third-party cost at cost)	2,500
Investigation administration fee (where permitted and imposed by decision)	5,000
Re-inspection following material non-compliance (per day, per	1,750

inspector)

5. Liquidity and escrow requirements (Schedule)

Applicants must demonstrate adequate financial resources, liquidity and safeguarding arrangements. Minimum requirements are set out below.

Licence class	Minimum liquidity / escrow requirement
All classes (A–E)	Maintain at all times liquid financial resources sufficient to meet (i) 3 months of projected fixed operating expenses; and (ii) anticipated wind-up costs. Liquid resources must be held in cash or cash equivalents with an eligible bank/custodian and must be unencumbered.
Class A – Exchange / marketplace-facing models	Liquidity coverage ratio (LCR): Liquid Assets ≥ (Client Fiat Payables + 3 months fixed operating expenses). Where client fiat is held, it must be held in segregated trust/escrow accounts. Daily reconciliation required.
Class B – Custody / wallet services	Operational liquidity: Liquid Assets ≥ 3 months fixed operating expenses. Client asset safeguarding: 100% segregation of client assets; key management controls; insurance (where available) commensurate with risk.
Class C – Transfer / payment services	Liquidity: Liquid Assets ≥ 2 months fixed operating expenses. If transmitting fiat or settling client balances, maintain settlement buffer and segregated accounts with daily reconciliation.
Class D – Stablecoin issuance / issuer arrangements (if permitted)	Reserve/escrow: 1:1 backing of 'specified stablecoin' liabilities by eligible reserve assets held in segregated custody/escrow accounts. Redemption liquidity: maintain a cash buffer to meet peak redemptions (minimum 10% of outstanding liabilities in cash or cash equivalents unless otherwise approved). Monthly reserve attestation; quarterly independent assurance.
Class E – Trading platform operator / order book	Liquidity: Liquid Assets ≥ 3 months fixed operating expenses. If interfacing with custody/settlement, comply with Class A/B safeguarding requirements as applicable.

6. VA-1: Application Form

Complete all Sections. Where not applicable, state "N/A". Provide attachments clearly labelled.

VA-1A Applicant details

Legal name of applicant (as incorporated): _____
Trading name(s): _____
Company number / registration number: _____
Registered office address: _____
Principal place of business: _____
Contact person (name, title): _____

Telephone / Email: _____
Website: _____

VA-1B Licence class selection (tick all that apply)

☐ Class A – Virtual Asset Exchange (Fiat-to-Virtual Asset): exchange between fiat currency and virtual assets.

☐ Class B – Virtual Asset Exchange (Virtual Asset-to-Virtual Asset): exchange between one or more virtual assets.

☐ Class C – Virtual Asset Transfer and Payment Services: transfer of virtual assets on behalf of another person and related payment services.

☐ Class D – Custody and Wallet Services: safekeeping or administration of virtual assets or instruments enabling control over virtual assets.

☐ Class E – Trading Platform Operator: operation of a virtual asset trading platform, marketplace or order book.

Attach the relevant Class Schedule(s) at Section 7 for each class selected.

VA-1C Business summary

Provide a concise description of the proposed business model, products/services, target clients, jurisdictions, and expected transaction flows.

VA-1D Governance and key persons

List directors, senior officers and key persons. Attach organisation chart and committee structure.

Name	Role	Resident in TCI? (Y/N)	Start date	VA-2 PQ attached?

VA-1E Ownership / controllers / beneficial owners

Provide full ownership structure. Identify controllers and beneficial owners (BOs). Attach group structure chart.

Person/Entity	Type (BO/Controller/ Shareholder)	% interest / control	Jurisdiction	Evidence attached

VA-1F Declarations and undertakings

Tick and sign the declarations in VA-6.

7. Class Schedules (attach only those that apply)

Schedule A (Class A – Virtual Asset Exchange)

Provide the following class-specific information and supporting documents:

-Market structure description (order types, matching, market surveillance).

-Listing policy (admission, ongoing monitoring, delisting).

-Client onboarding and disclosures; conflicts of interest policy.

Safeguarding model (custody in-house / third party); reconciliation procedures.

-Settlement model and fiat rails; bank/PSP letters of intent.

Schedule B (Class B – Custody and Wallet Services)

Provide the following class-specific information and supporting documents:

- Custody control framework; key management policy (HSM/MPC; key ceremony).

-Segregation of client assets; reconciliation and proof-of-reserves approach.

-Insurance arrangements (if any) and coverage summary.

-Hot/warm/cold wallet structure; access controls and audit logs.

-Outsourcing arrangements (if custody sub-contracted).

Schedule C (Class C – Transfer and Payment Services)

Provide the following class-specific information and supporting documents:

- Transfer rails and payment flow diagrams (VA and fiat).

- Settlement finality and reconciliation methodology.

- Safeguarding of fiat balances; escrow/trust account arrangements.

-Fraud controls, chargeback/dispute handling (where applicable).

-Sanctions screening and Travel Rule solution details.

Schedule D (Class D – Stablecoin Issuance / Issuer arrangements)

Provide the following class-specific information and supporting documents:

- Stablecoin design, backing/peg mechanism, issuance/redemption process.

-Reserve policy; eligible reserve assets; custody/escrow arrangements.

-Redemption policy and timelines; liquidity buffer plan.

-Disclosure (White Paper/terms); consumer risk disclosures.

-Independent assurance: attestation/audit plan and reporting cadence.

Schedule E (Class E – Trading Platform Operator)

Provide the following class-specific information and supporting documents:

- Platform design and rulebook; participant eligibility and onboarding.

-Market integrity controls (surveillance, abuse monitoring).

-Order book / trading rules; transparency and reporting.

-Custody/settlement interface and safeguarding controls.

-Business continuity and operational resilience plan.

8. VA-2: Personal Questionnaire (PQ) — to be completed by each relevant person

Attach one completed PQ per individual (directors, controllers, BOs, senior officers, MLRO, Compliance Officer, CTO where applicable).

Individual	Role	PQ attached (Y/N)

9. VA-3: AML/CFT/CPF Programme Schedule (summary checklist)

-Enterprise-wide ML/TF/PF risk assessment (virtual assets-specific).

- Customer due diligence programme (CDD/EDD), PEPs, source of funds/wealth.

-Travel Rule compliance (policy + solution provider + rule coverage).

-Sanctions screening (UN and domestic lists), screening frequency, alert handling.

- Transaction monitoring programme; typologies and red flags; STR reporting workflow.

-Recordkeeping and data retention; audit trail for VA transfers.

-Training plan and independent testing/audit of AML/CFT/CPF controls.

10. VA-4: Technology and Cybersecurity Schedule (summary checklist)

-System architecture and data flows; hosting locations; third-party dependencies.

-Cybersecurity framework and policies; access controls; vulnerability management.

-Key management (HSM/MPC) and segregation controls; privileged access logs.

-Incident response plan; incident notification capability; tabletop tests.

- Business continuity and disaster recovery (RTO/RPO); backup strategy.

- Penetration test report (recent, independent) or plan and timeline.

11. VA-5: Financial Resources, Liquidity and Safeguarding Schedule (summary checklist)

-Audited financial statements (if existing) or opening balance sheet (new entity).

- 3-year financial projections; assumptions; stress scenarios.

-Liquidity plan demonstrating compliance with Schedule in Section 5.

-Client asset safeguarding policy (segregation, reconciliation, escrow).

-Wind-up plan: triggers, funding, client asset return, communications plan.

12. VA-6: Declarations, Undertakings and Consents

Authorised signatory to complete below:

I/We certify that the information provided is true, complete and not misleading.

I/We consent to the Commission making such enquiries as it considers necessary, including fit and proper checks.

Name: _____ Title: _____

Signature: _____ Date: _____

Acronym Interpretations:

PSP – Payment Service Provider

An entity that provides services to process, initiate, or facilitate payment transactions, including those using virtual assets, on behalf of users. This term generally refers to organisations involved in payment processing, e-money services, digital wallets, gateways, and similar functions in the digital economy.

HSM/MPC – Hardware Security Module / Multi-Party Computation

HSM refers to dedicated physical cryptographic devices used to securely generate, store, and manage cryptographic keys and perform secure operations.

MPC refers to cryptographic techniques that distribute the computation of cryptographic operations across multiple parties so that no single party has access to the complete set of keys. Together, these technologies strengthen operational security in virtual asset custody and transaction signing.

DR/BCP – Disaster Recovery / Business Continuity Plan

Disaster Recovery (DR) is a documented strategy for restoring IT systems, applications, data, and operations after a major disruption.

Business Continuity Plan (BCP) is a broader organisational plan to ensure that critical business functions continue with minimal interruption during and after a disruptive event. Both are essential components of operational resilience for virtual asset service providers.

CTO – Chief Technology Officer

The senior executive responsible for overseeing technology strategy, governance, implementation, and risk management within an organisation. In the context of virtual assets, the CTO plays a key role in ensuring secure and compliant technology operations. (General industry term)

EDD – Enhanced Due Diligence

An elevated form of customer due diligence undertaken where there are higher risks of money laundering, terrorist financing or financial crime. EDD involves obtaining and verifying additional information, such as source of funds or wealth, and applying enhanced monitoring and reporting measures.

PEPs – Politically Exposed Persons

Individuals who hold, or have held, prominent public positions or functions (e.g., senior government officials, judges, senior military officers), as well as their family members and close associates. Due to

increased risk of corruption or misuse of public office for financial crime, PEPs require heightened scrutiny under AML/CFT measures.

RTO – Recovery Time Objective

The targeted maximum amount of time that a business process or system may be unavailable after a disruption before adverse consequences become unacceptable.

RPO – Recovery Point Objective

The targeted maximum amount of data loss measured in time that an organisation can tolerate during a disruption. It represents the point in time to which data must be restored for business operations to resume effective.

PASSED by Parliament this day of 2026.

…….	…….
Tracey Parker	**Gordon Burton**
Clerk of the Parliament	**Speaker**

INFORMATION AND COMMUNICATION TECHNOLOGY REGULATIONS

(Section 47)

ICT Operational Resilience

1. Issuers shall establish and maintain secure, resilient, recoverable and scalable ICT systems within the stablecoin ecosystem that conform to international ICT standards.

Access Control

2. (1) Issuers shall implement and maintain robust access management controls to ensure the confidentiality, integrity, and availability of all technical components within the stablecoin ecosystem.

(2) All privileged access to the stablecoin ecosystem shall be monitored for suspicious activity and alerts generated to appropriate personnel.

(3) Issuers shall ensure access to the stablecoin ecosystem is restricted to personnel role-specific needs, granted only after authorisation, and revoked immediately upon role termination, with automated enforcement and biannual audits.

Multi-Party Authorisation Controls

3. (1) Subject to subsection (2), no individual Person, or any automated system acting on behalf of a single person, shall have unilateral authority to execute, initiate, or approve any act concerned with the control and management of a stablecoin.

(2) An Issuer shall ensure that any act involved in the issuance, redemption, transfer, or other material control or management of a stablecoin or its reserve assets shall be subject to joint authorisation by no less than two Persons duly approved and appointed.

(3) The Commission may—

(a) require Tier 1 and Tier 2 Issuers to implement verifiable M-of-N threshold authorisation mechanisms, including multi-signature wallets or hardware-based approval protocols; or

(b) mandate or approve the use of M-of-N controls where critical functions (e.g. reserve access, systemic redemptions, or protocol updates) are involved, particularly for Tier 1 or systemic issuers.

(4) Where necessary, a qualified independent third party, such as a licensed custodian, external auditor, or trusted execution environment provider, may be required to verify or co-sign such authorisations for added assurance.

Key Management

4. (1) A licensed issuer shall implement secure key management practices to protect cryptographic keys used in the issuance, redemption, custody, or transfer of stablecoins.

(2) Key material shall be protected from unauthorised access while not in use.

(3) Stablecoin key material operations shall be conducted in a secure, audited environment free from unauthorised surveillance or access.

(4) Equipment shall be pre-checked for tampering, software and hardware updates, and other vulnerabilities, and physical and technical safeguards shall include restricted access and environmental controls.

(5) Stablecoin key material shall be backed up and stored in a separate location from primary key material operations and the key material backups shall be protected from unauthorised access and use and environmental impacts.

(6) All key material operations shall be documented, maintained and made known to relevant parties.

Wallet Security

5. (1) Issuers shall implement security controls for both custodial and non-custodial environments, including safeguards to prevent unauthorised access, protect private keys, and ensure the operational integrity of wallet systems.

(2) Issuers shall implement risk mitigation measures for both custodial and non-custodial wallets.

(3) Issuers shall store the majority of stablecoin reserves in secure, offline cryptographic storage systems isolated from internet-connected environments.

(4) Only operational amounts necessary for daily transactions may reside in internet-exposed systems, subject to strict access controls and real-time monitoring.

(5) Subject to Section 41, all transactions affecting stablecoin reserves or protocol governance, shall require authorisation from multiple authorised signers.

(6) The minimum required signer thresholds to conduct transactions affecting stablecoin reserves or protocol governance shall be determined through documented risk assessments.

Secure Coding Practices

6. (1) An issuer shall adopt and maintain secure software development and coding practices across all custom-built systems that support the issuance, governance, custody, or transfer of stablecoins.

(2) Issuers shall apply secure coding techniques to minimise vulnerabilities in custom software.

(3) Secure coding practices shall be reviewed periodically by the Issuer, and updated as necessary, having regard to industry-recognised standards.

Oracle Security

7. (1) Subject to subsection (2), Issuers shall ensure that all Oracles and external data sources integral to stablecoin issuance, redemption, or stability mechanisms are secure, reliable, and resilient to manipulation.

(2) Issuers shall implement redundancy measures, third-party audits of oracle systems, and real-time monitoring for anomalies to ensure compliance with the requirement in subsection (1).

Human Resource Security

8. (1) Issuers shall ensure that all personnel who can affect the confidentiality, integrity, and availability of the stablecoin ecosystem are aware of their roles and responsibilities and formally acknowledge them in writing.

(2) Issuers shall ensure each personnel under their control with access to the stablecoin ecosystem, undergo pre-employment and periodic background, criminal and identification checks conducted by approved third parties providers.

(3) Such checks shall assess integrity, criminal, and potential, contingent or real conflicts of interest, with exemptions permitted only where prohibited by applicable local law.

(4) Where local laws restrict background, criminal and identification checks, Issuers shall implement compensating controls to mitigate risks from unvetted personnel.

Technology and Cybersecurity Requirements

9. (1) Issuers shall ensure that only operational amounts necessary for daily transactions reside in internet-exposed systems, which shall be subject to strict access controls, multi-factor authentication, and real-time monitoring to detect and prevent unauthorised access or cyber intrusion;

(2) Issuers shall conduct cybersecurity assessments in accordance with templates prescribed by the Commission.

(3) The Commission may prescribe minimum technology and cybersecurity and assessment requirements as set out in Schedule 10 and 11.

Monitoring and Incident Response

10. (1) An issuer shall implement continuous monitoring systems and incident response protocols to identify, assess, and respond to operational disruptions, cybersecurity threats, or other incidents affecting stablecoin activities.

(2) Issuers shall implement real-time monitoring of relevant blockchain activity to detect anomalies affecting stablecoin reserves or protocol governance.

(3) Automated alerts shall trigger predefined response protocols, with incidents escalated to qualified personnel for investigation and remediation.

(4) Issuers shall establish an incident response management plan to address security breaches and operational system failures.

(5) Incident response teams shall be trained and conduct regular drills to test response effectiveness and cover threat scenarios identified from the ICT risk assessment.

(6) Issuers shall subscribe to and integrate intelligence feeds from qualified third-party providers to monitor current and emerging threats that could impact the security of the stablecoin ecosystem.

(7) Issuers shall implement systems to continuously identify, assess, treat, and monitor cybersecurity threats to the issuing platform, including the stablecoin smart contract infrastructure, reserve management systems, and user interfaces.

(8) Minimum systems required under subsection (4) shall include—

(a) event-based logging; and

(b) Smart Contract change detection; and

(c) anomaly alerting mechanisms.

(9) The level of monitoring shall be commensurate with the scale, complexity, and risk profile of the Issuer, and shall escalate proportionally with tiered classification under Section 13.

(10) The Commission may issue rules, guidance, or technical standards prescribing the minimum acceptable controls for each tier under this subsection.

Governance and Risk Management

11. (1) Issuers shall establish and maintain an ICT governance framework ensuring a documented ICT strategy with policies, standards, and procedures that enforce multi-layered ICT controls, continuous monitoring and improvement and align with international ICT standards.

(2) The minimum governance and risk management checklist requirements set out in Exhibit B apply to all tiered Issuers.

(3) Issuers shall implement a comprehensive ICT risk management framework.

(4) Issuers shall establish and maintain robust business continuity, disaster recovery, and resolution policies designed to ensure the uninterrupted provision of critical services in the event of cyberattacks, liquidity shortfalls, or critical system failures which must—

(a) be tested at least annually and include clearly defined recovery time objectives;

(b) provide for the use of redundant systems and infrastructure to minimise disruption;

(c) include contingency funding plans and liquidity management frameworks to address financial shocks; and

(d) align with internationally recognised standards for operational resilience and user fund protection.

(5) Issuers shall conduct appropriate due diligence and implement ongoing monitoring and periodic review of all third-party VASPs capable of affecting the integrity, security, operational resilience, or continuity of stablecoin issuance or related activities.

(6) Ongoing audits and assessments shall be conducted to ensure compliance with international ICT standards.

(7) For the purposes of Schedule 7, the technology and cybersecurity controls listed in Schedule 11 are considered baseline tiered requirements and may be supplemented by the Commission under Section 104.

VIRTUAL ASSETS BUSINESS (FEES) REGULATIONS

(Section 102)

General

1. (1) The Schedules of fees and penalties prescribed under the various Regulations of the Financial Services Commission Act as relates to financial businesses, are to be amended to include all fees prescribed under this Act, as appropriate —

(2) The Commission may prescribe—

(a) the amount of any fee;

(b) the manner, time and method of payment;

(c) different fees for different classes of authorisation, licence classes, stablecoin tiers, or risk profiles;

(d) reduced fees for sandbox authorisations, pilot programmes or innovations approved by the Commission;

(e) additional fees for late filings, re-inspections, special audits, skilled-person reports, enforcement monitoring, or other special supervisory actions;

(f) fee waivers or remissions in circumstances as prescribed by Regulations; and

(g) interest or administrative charges for late payment.

(3) Unless otherwise as prescribed by Regulations, fees are payable in United States dollars and are non-refundable.

(4) Regulations may prescribe how fees apply where an applicant seeks authorisation for more than one licence class—

Fee categories — VASP licence classes (Classes A–E)

2. The Commission shall prescribe application fees for each of the following licence classes—

A. Fees (USD) — summary

Licence class	Application fee Non-refundable	Grant / issuance fee	Annual supervisory fee

Class A (Virtual Asset Exchange)	7,500	20,000	20,000
Class B (Custody / Safekeeping / Wallet custody)	5,000	15,000	15,000
Class C – Virtual Asset Transfer and Payment Services	5,000	15,000	15,000
Class D (Stablecoin Issuance / Issuer arrangements)	10,000	25,000	25,000
Class E (Trading Platform Operation	3,750	12,500	12,500

Variation, approval and other administrative fee categories

3. The Commission shall prescribe fees for, among other things—

(a) renewal of a Full (perpetual) licence;

(b) variation of licence scope or licence class;

(c) approval of a change of controller or significant beneficial owner;

(d) approval of appointment or change of an authorised person, representative, MLRO, MLCO/natural person, senior officer or key function holder;

(e) approval of material outsourcing arrangements or custody arrangements;

(f) approval of a material change to technology systems (including core wallet, custody, settlement or Travel Rule systems);

(g) applications for exemptions, dispensations or extensions (where permitted); and

(h) copies, certified extracts, searches and other administrative services.

Recognition fee categories — smart contract auditor / assurance provider / recognised activity

4. The Commission shall prescribe fees for—

(a) application for recognition as a smart contract auditor or assurance provider;

(b) annual recognition/supervisory fees (where applicable); and

(c) renewal of recognition (where applicable).

Fee categories — stablecoin authorisations (Part 9)

5. (1) The Commission shall prescribe application fees and annual supervisory fees for stablecoin authorisations by stablecoin tier.

(2) Regulations may prescribe whether, and in what circumstances, stablecoin fees are payable in addition to fees under paragraphs 3 and 4.

(3) Regulations may prescribe additional fees for reserve audits/attestations, redemption testing, stress testing, or other enhanced supervisory actions applicable to issuers.

Regulatory Sandbox Fees (Part 8)

6. (1) The fees in this Schedule apply to applications for, and participation in, the Regulatory Sandbox established under Part 8.

(2) Unless otherwise provided, fees are payable at the time the relevant application, request or filing is submitted and are non-refundable.

(3) Quarterly monitoring fees are payable in advance for each quarter of sandbox participation.

(4) Where a sandbox participant transitions to a full VASP licence, 50% of the Sandbox Admission Fee paid under item 2 shall be credited against the VASP licence application fee (Schedule 1), provided that the full licence application is submitted within 6 months of sandbox completion.

(5) Sandbox fees apply in addition to any administrative and supervisory filing fees (Schedule 3) and do not limit the Commission's power to impose conditions, directions, or administrative monetary penalties.

Item	Matter	Fee (USD)
1	Sandbox application fee (payable on submission)	Class A: 2,500 | Class B: 2,000 | Class C: 2,000 | Class D: 1,500
2	Sandbox admission fee (payable on acceptance into the sandbox)	Class A: 5,000 | Class B: 4,000 | Class C: 4,000 | Class D: 3,000
3	Quarterly sandbox supervisory monitoring fee (payable per quarter)	Class A: 7,500 | Class B: 6,000 | Class C: 6,000 | Class D: 5,000
4	Extension of sandbox period (per extension request)	1,000
5	Material variation to testing plan / scope during sandbox (per request)	1,250
6	Exit and transition assessment (optional—where the Commission undertakes a formal	2,500

	transition review)	
7	Re-entry / second sandbox cohort application (where prior sandbox concluded without transition)	Same as item 1

EXPLANATORY MEMORANDUM

This Bill seeks to establish a comprehensive legal and regulatory framework for virtual asset business activities conducted in or from within the Turks and Caicos Islands.

The Bill provides for the licensing, regulation, supervision and enforcement of Virtual Asset Service Providers ("VASPs") and related virtual asset activities, including stablecoin issuance, virtual asset offerings, custody services, exchange services, transfer services, wallet services, token issuance activities, and other digital asset business activities.

The development of virtual assets and related financial technologies has created significant opportunities for innovation, investment, financial inclusion and economic development globally. At the same time, virtual asset activities present material risks relating to money laundering, terrorist financing, proliferation financing, cybercrime, fraud, consumer protection, market integrity, prudential stability and cross-border regulatory arbitrage.

The Bill is intended to ensure that the Turks and Caicos Islands maintains a modern, risk-based and internationally aligned framework for the regulation and supervision of virtual asset activities, while protecting the integrity and reputation of the Islands as an international financial services jurisdiction.

The Bill aligns the Turks and Caicos Islands with evolving international standards and best practices relating to virtual assets, including the recommendations and guidance issued by the Financial Action Task Force ("FATF"), the Financial Stability Board ("FSB"), the International Organization of Securities Commissions ("IOSCO"), and other international standard-setting bodies.

In particular, the Bill seeks to implement and support compliance with FATF Recommendation 15 relating to virtual assets and virtual asset service providers, including requirements relating to licensing, supervision, risk-based regulation, customer due diligence, sanctions compliance, suspicious transaction reporting and the FATF "Travel Rule".

The Bill further recognises the increasing international importance of stablecoins and other digital payment mechanisms and establishes a dedicated regulatory framework for stablecoin issuance, reserve management, governance, redemption rights, disclosure obligations and prudential safeguards.

The Bill adopts a technology-neutral and activity-based approach to regulation, recognising that regulation should focus on the nature of the financial activity and the risks arising from such activity, rather than on the underlying technology itself.

The Bill also seeks to support responsible innovation through the establishment of a regulatory sandbox framework that permits controlled testing of innovative products, services and business models under the supervision of the Financial Services Commission.

The Bill is intended to support innovation while ensuring that virtual asset activities are conducted in a safe, transparent and well-regulated manner that protects consumers, safeguards market integrity, mitigates money laundering and terrorist financing risks, and protects the reputation and financial stability of the Turks and Caicos Islands.

PART I sets out the preliminary provisions, including interpretation, scope and application of the Act, and clarifies the relationship between this Act and other financial services legislation.

PART II designates the Financial Services Commission as the competent authority responsible for the regulation, supervision and enforcement of VASPs and virtual asset activities in or from within the Islands.

PART III establishes the licensing framework for VASPs, including licensing requirements, fit and proper assessments, prudential requirements, governance obligations, outsourcing arrangements, and supervisory oversight.

PART IV sets out the ongoing obligations applicable to licensed VASPs, including requirements relating to governance, safeguarding of customer assets, market conduct, disclosures, complaints handling, business continuity, operational resilience, and custody arrangements.

PART V establishes AML/CFT/CPF obligations applicable to VASPs and incorporates FATF Recommendation 15 and Recommendation 16 obligations, including requirements relating to the FATF Travel Rule and virtual asset transfer requirements.

PART VI regulates initial virtual asset offerings and issuance activities, including disclosure obligations, White Paper requirements, marketing restrictions, and civil liability for misstatements.

PART VII establishes requirements relating to information and communication technology systems, cybersecurity, operational resilience,

incident reporting, systems assurance, outsourcing, and cross-border interoperability.

PART VIII provides for the establishment and operation of a regulatory sandbox to support responsible innovation under controlled supervisory conditions.

PART IX establishes a dedicated regulatory framework for stablecoins, including licensing, reserve management, governance, prudential requirements, redemption rights, disclosure obligations, reserve attestation, reserve segregation, and operational resilience requirements.

PART X establishes customer and user protection provisions, including fraud prevention and redress mechanisms.

PARTS XI and XII establish supervisory, investigative, enforcement and appeals mechanisms, including administrative penalties, directions, court orders, freezing orders, insolvency-related measures, offences and sanctions.

PART XIII contains miscellaneous provisions relating to regulations, fees, transitional provisions, amendment of Schedules, review of the Act, and related matters.

The Bill also includes Schedules setting out licensing criteria, stablecoin reserve requirements, technology and cybersecurity standards, sandbox requirements, guidance principles, and consequential amendments.